4910-15-U

DEPARTMENT OF HOMELAND SECURITY

COAST GUARD

33 CFR Parts 101 and 102

[USCG-2003-14792]

RIN 1625-AA69

Implementation of National Maritime Security Initiatives

AGENCY: Coast Guard, DHS.

ACTION: Temporary interim rule with request for comments and notice of meeting.

SUMMARY: The Coast Guard has published a series of six interim rules in today's Federal Register to promulgate maritime security requirements mandated by the Maritime Transportation Security Act of 2002. The six interim rules consist of: Implementation of National Maritime Security Initiatives; Area Maritime Security; Vessel Security; Facility Security; Outer Continental Shelf Facility Security; and Automatic Identification System. In addition to the Automatic Identification System interim rule, we have issued a separate request for comments for further expanding the implementation of the Automatic Identification System. The series of interim rules addresses security assessments and plans, as well as other

security standards, measures, and provisions that, with the exception of Automatic Identification System, will be codified in the new subchapter H of Title 33 of the Code of Federal Regulations.

This interim rule, the Implementation of National Maritime Security Initiatives, establishes the general regulations for subchapter H. It does so by providing a comprehensive discussion of industry-related maritime security requirements and a summary of the cost and benefit assessments of the entire suite of interim rules. The alignment of domestic maritime security requirements with the International Ship and Port Facility Security Code and recent amendments to the International Convention for the Safety of Life at Sea is also addressed here.

The discussions provided within each of the other five interim rules are limited to the specific requirements they contain.

DATES:

Effective date. This interim rule is effective from [Insert date of publication in the FEDERAL REGISTER.] until November 25, 2003. On [Insert effective date of publication in the FEDERAL REGISTER.], the Director of the Federal Register approved the incorporation by reference of certain publications listed in this rule.

Comments. Comments and related material must reach the Docket Management Facility on or before [Insert date 30 days after date of publication in the FEDERAL REGISTER.]. Comments on collection of information sent to the Office of Management and Budget (OMB) must reach OMB on or before [Insert date 30 days after date of publication in the FEDERAL REGISTER.].

Meeting. A public meeting will be held on July 23, 2003, from 9 a.m. to 5 p.m., in Washington, D.C.

ADDRESSES:

Comments. To ensure that your comments and related material are not entered more than once in the docket, please submit them by only one of the following means:

(1) Electronically to the Docket Management System at http://dms.dot.gov.

(2) By mail to the Docket Management Facility (USCG-2003-14792) at the U.S. Department of Transportation, room PL-401, 400 Seventh Street SW., Washington, DC 20590-0001.

(3) By fax to the Docket Management Facility at 202-493-2251.

(4) By delivery to room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday,

except Federal holidays. The telephone number is 202-366-9329.

You must also mail comments on collection of information to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street NW., Washington, DC 20503, ATTN: Desk Officer, U.S. Coast Guard.

Meeting. A public meeting will be held on July 23, 2003 in Washington, D.C. at the Grand Hyatt Washington, D.C., 1000 H Street, N.W., Washington, D.C. 20001.

Availability. You may inspect the material incorporated by reference at room 2110, U.S. Coast Guard Headquarters, 2100 Second Street SW., Washington, DC 20593-0001 between 8 a.m. and 4 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-267-0257. Copies of the material are available as indicated in the "Incorporation by Reference" section of this preamble.

FOR FURTHER INFORMATION CONTACT: If you have questions on this rule, call Commander Suzanne Englebert (G-M-1), U.S. Coast Guard by telephone 202-267-1103, toll-free telephone 1-800-842-8740 ext. 7-1103, or by electronic mail msregs@comdt.uscg.mil. If you have questions on viewing or submitting material to the docket, call Dorothy Beard,

Chief, Dockets, Department of Transportation, telephone 202-366-5149.

SUPPLEMENTARY INFORMATION:

Due to the short timeframe given to implement these National Maritime Transportation Security initiatives, as directed by the Maritime Transportation Security Act (MTSA) of 2002 (MTSA, Public Law 107-295, 116 STAT. 2064), and to ensure all comments are in the public venue for these important rulemakings, we are not accepting comments containing protected information for these interim rules. We request you submit comments, as explained in the Request for Comments section below, and discuss your concerns or support in a manner that is not security sensitive. We also request that you not submit proprietary information as part of your comment.

The Docket Management Facility maintains the public docket for this rulemaking. Comments and material received from the public, as well as documents mentioned in this preamble as being available in the docket, will be available for inspection or copying at room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet at http://dms.dot.gov.

Electronic forms of all comments received into any of our dockets can be searched by the name of the individual submitting the comment (or signing the comment, if submitted on behalf of an association, business, labor unit, etc.) and is open to the public without restriction. You may also review the Department of Transportation's complete Privacy Act Statement published in the Federal Register on April 11, 2000(65 FR 19477-78), or you may visit http://dms.dot.gov/.

Request for Comments

We encourage you to participate in this rulemaking by submitting comments and related material. Your comments will be considered for the final rule we plan to issue before November 25, 2003, to replace this interim rule. If you choose to comment on this rule, please include your name and address, identify the specific docket number for this interim rule (USCG-2003-14792), indicate the specific heading of this document to which each comment applies, and give the reason for each comment. If you have comments on another rule please submit those comments in a separate letter to the docket for that rulemaking.

You may submit your public comments and material electronically, by fax, by delivery, or by mail to the Docket Management Facility at the address under ADDRESSES.

Please submit your public comments and material by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period.

Public Meetings

We will hold a public meeting on July 23, 2003, in Washington, D.C. at the Grand Hyatt Hotel, at the address listed under ADDRESSES. The meeting will be from 9 a.m. to 5 p.m. to discuss all of the maritime security interim rules, and the Automatic Identification System (AIS) interim rule, found in today's Federal Register. In addition, you may submit a request for other public meetings to the Docket Management Facility at the address under ADDRESSES explaining why another one would be beneficial. If we determine that other meetings would aid this rulemaking, we will hold them at a time and place announced by a later notice in the Federal Register.

Regulatory Information

We did not publish a notice of proposed rulemaking (NPRM) for this rulemaking and are making this rule

effective upon publication. Section 102(d)(1) of the MTSA requires the publication of an interim rule as soon as practicable without regard to the provisions of chapter 5 of title 5, U.S. Code (Administrative Procedure Act). The MTSA also states that any interim rule issued to implement its provisions shall expire on November 25, 2003, unless it has been superseded by a final regulation. The Coast Guard finds that harmonization of U.S. regulations with maritime security measures adopted by the International Maritime Organization (IMO) in December 2002, and the need to institute measures for the protection of U.S. maritime security as soon as practicable, furnish good cause for this interim rule to take effect immediately under both the Administrative Procedure Act and section 808 of the Congressional Review Act.

Background and Purpose

In the aftermath of September 11, 2001, the Commandant of the Coast Guard reaffirmed the Coast Guard's Maritime Homeland Security mission and its lead role — in coordination with the Department of Defense; Federal, State, and local agencies; owners and operators of vessels and marine facilities; and others with interests in our nation's Marine Transportation System — to detect, deter, disrupt, and respond to attacks against U.S. territory,

population, vessels, facilities, and critical maritime infrastructure by terrorist organizations.

In November 2001, the Commandant of the Coast Guard addressed the IMO General Assembly, urging that body to consider an international scheme for port and shipping security. Recommendations and proposals for comprehensive security requirements, including amendments to International Convention for Safety of Life at Sea, 1974, (SOLAS) and the new ISPS Code, were developed at a series of intersessional maritime security work group meetings held at the direction of the IMO's Maritime Safety Committee.

The Coast Guard submitted comprehensive security proposals in January 2002 to the intersessional maritime security work group meetings based on work we had been coordinating since October 2001. Prior to each intersessional meeting, the Coast Guard held public meetings as well as coordinated several outreach meetings with representatives from major U.S. and foreign associations for shipping, labor, and ports. We also discussed maritime security at each of our Federal Advisory Committee meetings and held meetings with other Federal agencies having security responsibilities.

In January 2002, the Coast Guard also held a two-day public workshop in Washington, DC, attended by more than 300 individuals, including members of the public and private sectors, and representatives of the national and international marine community (66 FR 65020, December 17, 2001; docket number USCG-2001-11138). Their comments indicated the need for specific threat identification, analysis of threats, and methods for developing performance standards to plan for response to maritime threats. Additionally, the public comments stressed the importance of uniformity in the application and enforcement of requirements and the need to establish threat levels with a means to communicate threats to the Marine Transportation System.

At the Marine Safety Committee's 76th session and subsequent discussions internationally, we considered and advanced U.S. proposals for maritime security that took into account this public and agency input. The Coast Guard considers both the SOLAS amendments and the ISPS Code, as adopted by IMO Diplomatic Conference in December 2002, to reflect current industry, public, and agency concerns. The entry into force date of both the ISPS Code and related SOLAS amendments is July 1, 2004, with the exception of the Automatic Identification System (AIS) whose implementation

for vessels on international voyages was accelerated to no later than December 31, 2004, depending on the particular class of SOLAS vessel.

Domestically, the Coast Guard had previously developed regulations for security of large passenger vessels that are contained in 33 CFR parts 120 and 128. Complementary guidance can be found in Navigation and Vessel Inspection Circular (NVIC) 3-96, Change 1, Security for Passenger Vessels and Passenger Terminals. Prior to development of additional regulations, the Coast Guard, with input from the public, needed to assess the current state of port and vessel security and their vulnerabilities. As mentioned previously, to accomplish this, the Coast Guard conducted a public workshop January 28—30, 2002, to assess existing Marine Transportation System security standards and measures and to gather ideas on possible improvements. Based on the comments received at the workshop, the Coast Guard cancelled NVIC 3-96 (Security for Passenger Vessels and Passenger Terminals) and issued a new NVIC 4-02 (Security for Passenger Vessels and Passenger Terminals), developed in conjunction with the International Council of Cruise Lines, that incorporated guidelines consistent with international initiatives (the ISPS Code and SOLAS). Additional NVICs were also published to further guide

maritime security efforts, including NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports), NVIC 10-02 (Security Guidelines for Vessels); and NVIC 11-02 (Security Guidelines for Facilities). The documents are available in the public docket (USCG-2002-14069) for review at the locations under ADDRESSES.

On November 25, 2002, President George W. Bush signed into effect Public Law 107-295, MTSA, 2002, which had been proposed to Congress the year before as the Port and Maritime Security Act (S. 1214). The MTSA requires the Secretary to issue an interim rule, as soon as practicable, as a temporary regulation to implement the Port Security section of the Act. The MTSA expressly waives the requirements of the Administrative Procedure Act, including notice and comment, for this purpose.

Nevertheless, the Coast Guard, in coordination with other agencies of the Department of Homeland Security (DHS) (e.g., the Transportation Security Administration (TSA)) and the Department of Transportation (e.g., the Maritime Administration (MARAD)), held seven public meetings in areas of high maritime interest to engage the public in discussions about the impact of its maritime security requirements. Prior to issuing this interim rule, the

Coast Guard wanted to receive preliminary comments that helped to structure the rulemakings published today. The seven public meetings were announced in a "notice of meeting; request for comment" document that was published in the Federal Register on December 20, 2002(67 FR 78742). The comprehensive notice of meeting requested comments addressing 40 issues as well as comments on the concepts presented in the ISPS Code and the MTSA. Comments made during the public meetings and those submitted to the public docket are available in the public docket (USCG-2002-14069) for review at the locations under ADDRESSES. A discussion of these comments is contained in this preamble under the Discussion of Comments to Maritime Security Public Meetings. The Coast Guard plans to publish a final rule by November 2003. This date is critical to meeting the timeline set in the MTSA for finalizing these security requirements. It is just as critical in order to uniformly implement the ISPS Code and SOLAS amendments.

To comply with the mandates of the MTSA, the Coast Guard is implementing portions of section 102 of the MTSA (46 U.S.C. sections 70102, 70103b through 70103d, 70104, 70114, and 70117) through this and a series of five other interim rules published elsewhere in today's Federal Register. Within this common preamble, we will generally

discuss each of the six interim rules. This common preamble will also discuss the National Maritime Transportation Security Plan, found in 46 U.S.C. 70103a, transportation security cards, found in 46 U.S.C. 70105, and foreign port assessments, found in 46 U.S.C. 70108, as they relate to the requirements established in the six interim rules.

Organization

As already stated, we have segmented the maritime security regulations into six separate interim rules. The entire series of rulemakings establishes a new subchapter H, containing six new parts, in Title 33 of the Code of Federal Regulations. For the ease of reading and comprehension, the rulemakings were written to highlight each segment of the maritime community and structured based on the organization of the regulations rather than in one single interim rule. A brief description of each of the six interim rules follows:

1. Implementation of National Maritime Security Initiatives. This general discussion includes the introduction of the new subchapter H into Title 33 of the Code of Federal Regulations. It also discusses the General Provisions within part 101 of that subchapter, and reserves part 102 for the National Maritime Security plan and

Advisory Committee requirements. This discussion covers the overall methodology we used to determine the appropriate application of security measures in accordance with the MTSA. A summary of the costs and benefits associated with implementing security requirements used for subchapter H are presented as well as a discussion of the security-related benefit for AIS. The requirements set out in this interim rule include the definitions for the entire subchapter and the provisions that pertain to all parts. It is strongly recommended that this interim rule be read prior to consulting one or more of the other specific parts or the AIS interim rule, which are published elsewhere in today's Federal Register, to ensure terms and applicability issues are understood. Additionally, the preamble to this interim rule includes a discussion of the comments made during the public meetings held on Maritime Security in January and February of 2003 and the comments submitted to the docket [USCG-2002-14069] that were received by February 28, 2003. All comments received after February 28, 2003, will be considered prior to the issuance of the final rules.

2. Area Maritime Security (AMS). The discussion in the preamble of the "Area Maritime Security" (USCG-2003-14733) interim rule found elsewhere in today's Federal

Register relates to the provisions within part 103 of subchapter H. Discussions about cost and benefit assessment for the Area Maritime Security regulations are also found in the Area Maritime Security preamble.

3. Vessel Security. The discussion in the preamble of the "Vessel Security" (USCG-2003-14749) interim rule found elsewhere in today's Federal Register relates to the provisions within part 104, titled Vessel Security, of subchapter H. It also includes a discussion of the additional parts of 33 CFR and 46 CFR amended or revised by the Vessel Security interim rule. Discussions about cost and benefit assessments for the vessel security regulations are found in the preamble of the interim rule "Vessel Security.". Consistent with customary international law, the requirements in part 104 do not apply to vessels engaged in innocent passage through the territorial sea of the U.S. or in transit passage through the navigable waters of the U.S. that form part of an international strait.

4. Facility Security. The discussion in the preamble of the "Facility Security" (USCG-2003-14732) interim rule found elsewhere in today's Federal Register relates to the provisions within part 105, titled Facility Security, of subchapter H. Discussions about cost and benefit

assessments for the facility security regulations are found in the preamble of the interim rule "Facility Security."

5. Outer Continental Shelf (OCS) Facility Security. The discussion in the preamble of the "Outer Continental Shelf Facility Security" (USCG-2003-14759) interim rule found elsewhere in today's Federal Register relates to the provisions within part 106, titled "Outer Continental Shelf Facility Security," of subchapter H. Discussions about cost and benefit assessments for the OCS facility security regulations are found in the preamble of the interim rule "Outer Continental Shelf Facility Security."

6. Automatic Identification Systems (AIS). The discussion in the preamble of the "Automatic Identification System; Vessel Carriage Requirement" (USCG-2003-14757) interim rule found elsewhere in today's Federal Register relates to the provisions within 33 CFR parts 26, 161, 164, and 165. These requirements relate to the fitting of AIS on certain vessels as mandated in 46 U.S.C. 70114 and MTSA section 102(e). Discussions about cost and benefit assessments for the AIS regulations with respect to both safety and security are found in the preamble of the interim rule "Automatic Identification System; Vessel Carriage Requirement."

Coordination with the SOLAS Requirements

For each interim rule, the requirements of the MTSA Section 102 align, where appropriate, with the security requirements embodied in the SOLAS amendments and the ISPS Code; however, the MTSA has broader application that includes domestic vessels and facilities. Thus, where appropriate, the Coast Guard intends to implement the MTSA through the requirements in the SOLAS amendments and the ISPS Code, parts A and B, for all vessels and facilities that are currently required to meet SOLAS, as well as those vessels on international voyages that fall below the mandated 500 gross tonnage, ITC (International Convention on Tonnage Measurement of Ships, 1969 (ITC)) threshold and facilities that are at risk of being involved in a transportation security incident. Further discussion on this risk and how we developed and assessed it for the maritime community is presented in the Applicability of National Maritime Security Initiatives discussion in this preamble.

In aligning the MTSA Section 102 requirements with the SOLAS amendments and the ISPS Code security requirements, we consider that the implementation of these requirements is best done through mandating compliance with the SOLAS amendments and the ISPS Code. The Coast Guard considers ISPS Code, part B, an essential element to ensure full and

effective compliance with the intent of the MTSA. Foreign flag vessels entering the U.S. will be expected to carry valid International Ship Security Certificates (ISSC) and have the security plans fully implemented. The relevant provisions in ISPS Code, part B, will be taken into account by Port State Control Officers to assess if the security plan is fully implemented as required by the interim rules found elsewhere in today's Federal Register. The flag administration may also choose to provide a document or endorsement to the ISSC to verify that the security plan was based upon full compliance with the relevant provisions of ISPS Code, part B, to assist Coast Guard Port State Control Officers. We intend to implement strong Port State Control measures to aggressively enforce these regulations that will include tracking the performance of all owners, operators, flag administrations, recognized security organizations, charterers, and port facilities. Noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port or significant delay. We will strictly enforce compliance with SOLAS and the ISPS Code for foreign SOLAS vessels, including assessing the risks posed by such vessels and any control measures that may be required when they call on foreign port facilities that do not comply

with SOLAS and the ISPS Code, and we will similarly ensure that other vessels or port facilities covered by these regulations meet the requirements of this subchapter. A vessel's or port facility's history of compliance, or lack thereof, or security incidents involving a vessel or port facility, will be important factors in determining what actions are deemed appropriate by Coast Guard Port State Control Officers to ensure that maritime security is preserved. As mentioned, the performance of the owner, operator, flag administration, recognized security organization, charterer, or port facility related to maritime security will also be some of the other factors that will be considered for the enforcement of maritime security in the U.S.

In addition to tracking performance, the Coast Guard's Port State Control program will also closely scrutinize an Administration's designation of recognized security organizations to ensure that those organizations fully meet the competencies and qualifications in the ISPS Code. Vessels with International Ship Security Certificates issued by recognized security organizations that are not properly designated, or that do not meet the required competencies and qualifications, will be subject to strict control measures, including possible expulsion from port

and denial of entry into the United States. Therefore, it is imperative that Administrations carefully evaluate an organization through a rational process, adhering to the stringent criteria in the ISPS Code and any future standards that are developed by IMO, before designating the organization as a recognized security organization and delegating certain security functions to it.

The requirements for the AIS interim rule found elsewhere in today's Federal Register align with the recent amendments to SOLAS Chapter V, Regulation 19 that were adopted during the IMO Diplomatic Conference in December 2002 and the MTSA (specifically, MTSA sec. 102(e) and 46 U.S.C. 70114).

Impact on Existing Domestic Requirements

Many current requirements for security exist that are impacted by the interim rules published in today's Federal Register. 33 CFR part 120, Security of Vessels, and 33 CFR part 128, Security of Passenger Terminals, currently exist but apply only to certain cruise ships. We do not intend to revise 33 CFR parts 120 or 128 in the Vessel Security interim rule found elsewhere in today's Federal Register. However, in the future, this part may be revised or entirely deleted. This will consolidate the security requirements for all vessels in subchapter H. If this

change to 33 CFR part 120 is made, foreign vessels that are required to comply with part 120 will be required to meet the requirements of part 104 including § 104.295 Additional requirements – Cruise Ships and passenger terminals that are required to comply with part 128 will be required to meet part 105.

The requirements in the interim rules also refer to and amend certain parts of 46 CFR and 49 CFR to ensure certificate of inspection requirements and other sections pertaining to facilities will include the new subchapter H requirements.

Notice of arrival requirements found in 33 CFR 160 have also been amended in the Vessel Security interim rule found elsewhere in today's Federal Register to ensure security-related information is provided to appropriate authorities prior to a vessel's entry into port. Additionally, the Captain of the Port (COTP) authorities within 33 CFR have been revised to ensure security-related elements and authorities are clearly highlighted.

Applicability of National Maritime Security Initiatives

As required in section 102 of the MTSA (46 U.S.C. section 70102a), the Coast Guard conducted an assessment of vessel types and U.S. facilities on or adjacent to the waters subject to the jurisdiction of the U.S. to identify

those vessel types and U.S. facilities that pose a high risk of being involved in a transportation security incident. The MTSA defines a transportation security incident as a security incident resulting in a significant loss of life, environmental damage, a disruption to the transportation system, or economic disruption in a particular area.

Method of Assessment.

In October 2001, the U.S. Coast Guard urgently needed to prioritize vessels and facilities based on the vulnerabilities to potential security threats and the consequences of potential incidents. We used a systematic, scenario-based process known as Risk-Based Decision Making (RBDM) to meet those needs. RBDM ensured a comprehensive evaluation by considering the relative risks of various target and attack mode combinations or scenarios. This provided a more realistic estimation of risk (and more efficient risk management activities) than a simple "worst-case outcome" assessment where only the worst possible consequences were considered.

In addition, the RBDM approach was based on the recommendations from the U.S. General Accounting Office (GAO). Managing risk is one of the best tools to complete a security assessment and to determine appropriate security

measures (GAO-01-822). The GAO recommended a comprehensive security threat and risk assessment process (GAO-01-1158T).

Another GAO report, Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts, illustrated a scenario-based, risk management approach as used within the private sector. This GAO report explained how a company successfully created a security plan using a risk-based approach. Like the company described in the GAO report, the Coast Guard's approach to commercial maritime security featured the systematic development and consideration of potential scenarios of concern. The generation of scenarios ensured completeness of the risk-based method (GAO/NSIAD-98-74).

Principles of Risk Management.

Risk management principles acknowledge that while risk generally cannot be eliminated, it can be reduced. Risk reduction is done by adjusting operations to reduce consequences, threats, or vulnerability of a security threat (consequences, threats and vulnerability will be discussed later in this document). Generally, it is easier to reduce vulnerabilities by adding security measures than to reduce consequences or threats (although reductions in all three are possible).

Risk assessments provide visibility into those elements of the risk equation that exert the greatest influence on risk. Those elements become the priorities in the risk management approach. The goal for maritime security is to ensure that if the level of threat increases, either the consequences or vulnerabilities decrease enough to offset that increase.

Process of Developing Maritime Security Risk Assessments.

First, to look at risk from the port level, local experts in the area of commercial maritime safety and security met with a team of professional risk consultants. Together we developed the Port Security Risk Assessment Tool (PS-RAT). The PS-RAT was provided to local authorities to evaluate vessels, facilities and infrastructure within their areas of responsibility for a variety of threat scenarios. The approach used for the PS-RAT was as previously described and advocated by GAO, where risk was assessed in terms of threat, vulnerability and consequence. The PS-RAT was initially implemented Coast Guard wide on 16 November 2001 and the individual COTPs completed baseline risk assessments on vessels, facilities, and infrastructure within their area of responsibility. Nationwide, the local assessors evaluated nearly 5200

scenarios on more than 2000 unique assets and infrastructure elements.

Second, at the area level, regional Coast Guard and other maritime experts in the area of commercial maritime safety and security compiled and analyzed the local level PS-RAT results to gain a better understanding of the security risks affecting their Coast Guard Districts and Areas. This assessment identified some recurring scenarios and common issues that needed to be addressed beyond the local level. It also helped clarify the need for another tool with a wider perspective that would be capable of evaluating risks at the national level.

Because of the local, relative nature of these assessments the PS-RAT did not support the national comparisons that were necessary for strategic planning. To accomplish strategic planning at the national level, a third team of Coast Guard subject matter and risk experts produced the National Maritime Homeland Security Risk Assessment Tool. Referred to in maritime circles as the National Risk Assessment Tool (N-RAT), the N-RAT provided a foundation for risk-based prioritization and subsequent regulatory assessment closely aligned with the guidance on conducting security risk assessments recommended by the GAO (GAO/NSIAD-98-74, GAO-02-150T, GAO-03-616T). The results

of the N-RAT provided a national evaluation of the relative security risk facing the Marine Transportation System of the U.S. The experts compared the results from the national assessment with the previously performed local assessments (PS-RAT) to ensure that consistent assumptions were made and that comparable measures of risk were produced.

What was Assessed.

The Coast Guard used the N-RAT to determine risks associated with specific threat scenarios against various classes of targets within the Marine Transportation System. The targets considered included vessels, facilities, waterways, and marine-related transportation systems. This allowed the Coast Guard to systematically consider all segments of the commercial maritime community to evaluate their potential for being involved in a transportation security incident.

Maritime Security Incident Scenarios.

The scenarios considered each element within the maritime community with respect to three general exposures:
Susceptibility as a target;
Use as a means of transferring or enabling the transfer of terrorists or terrorism-related materials; and
Use of vessel or facility as a weapon.

The three above-mentioned general threat scenarios integrate multiple circumstances considered as specific attack modes. That is, there are subordinate scenarios under each general scenario. For example in the basic threat scenario of "susceptibility as a target", a "boat loaded with explosives exploding alongside a docked tank vessel" is one attack mode while "tank vessel being commandeered and intentionally damaged" is another.

The N-RAT included over 50 target classes and 12 specific attack modes. This resulted in a matrix consisting of over 600 possible target/attack scenarios. Next, the 600 scenarios were screened for credibility by the expert panel. The credibility of a threat was based on the plausibility of an enemy actually carrying out the attack mode. For example, the "use as a means of transferring or enabling the transfer of terrorists or terrorism-related materials;" scenarios were screened out as "not credible attack modes" for military targets due to the inherent security measures in place. However, external attacks on these same targets were considered to be credible and were evaluated by the team. To balance comprehensiveness with efficiency, all scenarios were considered but only those scenarios deemed credible by the expert panel were further evaluated for risk.

Each credible threat scenario was evaluated by the panel of experts to determine the risk associated with a given attack against a specific target. The evaluation is based on a model showing the possible outcomes from any potential transfer or attack mode. Using previously cited GAO guidance in this area; the N-RAT risk was modeled as a function of the threat, vulnerability and consequences associated with each target/attack scenario. Each element is explained in the following sections. We realize that the terms used to identify each element may have recognized meanings in other contexts. In order to reduce confusion, we have included, as the first sentence in each element's discussion, the meaning associated with these terms for the purposes of the N-RAT.

Threat.

The term "threat" is a measure of the likelihood of an attack. It represents the perceived probability of an attack based on maritime domain awareness and the existence of intelligence.

Within the N-RAT, five threat levels were identified. The threat magnitude was described, and scoring benchmarks were provided for each level. Each benchmark of threat intensity was assigned a probability of occurrence for use in risk calculations. For each scenario, the experts

estimated the threat associated with an attack after considering the intent of hostile groups, prior security incidents, the capability to carry out the attack mode and any intelligence that indicated an organization was planning an attack. Lacking specific, credible intelligence that would allow an increase or reduction in the threat score for a specific attack mode, this was fixed at a constant value consistent with the Maritime Security (MARSEC) Levels previously established by the Coast Guard. The baseline assumption was that terrorist cells were operating with unknown targets and methods of attack. Changes in MARSEC Levels or specific, credible intelligence would trigger an appropriate modification in threat.

Vulnerability.

The term "vulnerability" measures the conditional probability of success given that a threat scenario occurs. It evaluates the adequacy and effectiveness of safeguards (both existing and proposed).

For the N-RAT, an attack was estimated as likely to succeed only if:

the target was available,

the target was physically accessible to be attacked,

organic security associated with the target would not detect and defeat the intended attack, and

the mode of attack would be capable of producing the intended consequences by overcoming the inherent safeguards designed into the system.

If all of the above mentioned barriers fail to halt the intended attack, then the attack would result in one or more outcomes. Outcomes ranged from relatively minor to catastrophic levels. The above mentioned four elements described the targets' overall vulnerability and were scored by the expert team.

The availability of a target measured its presence and predictability as it relates to an enemy's ability to plan and conduct an attack. The accessibility of a target, evaluated its physical deterrence (i.e., location, perimeter fencing, etc.) against different attack modes. It related to physical and geographic barriers that deter the threat without organic security. Organic security of a target assessed the ability of the target's security measures to deter the attack. It included security plans, communication capabilities, guard forces, intrusion detection systems, and ability of outside law enforcement to prevent the attack. Target hardness was a measure of the ability of a target to withstand attack. It is based on the complexity of target design and material construction characteristics.

Each vulnerability type was scored over five levels of magnitude (1-5 –lowest to highest). Again, scoring benchmarks were used to help ensure consistency. Each level of magnitude in every vulnerability category was assigned a probability of allowing an attack mode to proceed. The probability for each vulnerability category was factored, along with the threat probability, in risk calculations to determine the probability term of the risk equation. The individual probabilities were then multiplied together to derive the overall probability assessment for the target/attack scenario under consideration.

Consequence.

The term "consequence" is the estimation of adverse effect from the target/attack scenario and is an important consideration in risk evaluation and security planning. Six categories of effects were considered in evaluating the consequence of an attack: death/injury, economic, environmental, national defense, symbolic effect, and secondary (follow-on) national security threat. Inherent in this consideration was the criticality of the target. For each effect category, five levels of severity were described, and scoring benchmarks are provided. Unlike vulnerability, each severity level was assigned a common

consequence value for use in risk calculations. For example, the most severe economic impact consequences were considered equivalent to the most severe death/injury and symbolic effect consequences. The selected level for each factor was then converted to a representative value of potential loss for the consequence factor. These consequence scores were then summed across all appropriate categories to develop the consequence values for the target/attack scenario combination.

The estimated probability and consequence values were multiplied to calculate the overall risk for each target/attack scenario. This is essentially an estimate of the expected losses should a specific target/attack scenario occur.

Assessment Results.

The following graph is a demonstration of the type of the relative-risk results the N-RAT gave. Specific results, including scores, have been designated as sensitive security information (SSI). This graph simply displays the relationship between some types/classes of vessels and facilities or port infrastructure based on their relative risk. In each line, the parenthetical (I) and (D) stands for “international” or “domestic,” respectively.

[insert camera ready Table 1]

The below is a summary of the application requirements for these interim rules based on the N-RAT results:

Applicability Evaluation for Ports

The N-RAT results focused on individual vessel types and facilities subject to the authority of the Coast Guard. Scenarios were also developed that involved port transportation infrastructure that is vital to the port communities such as bridges, channel openings, and tunnels. This evaluation led to the conclusion that many structures within a port are also at risk of a transportation security incident and therefore should be covered by security measures. Therefore, we determined it would be appropriate to include specific guidance in part 103 to have the Area Maritime Security (AMS) Plan address these types of transportation infrastructure as well as those smaller vessels or facilities that fall below the transportation security incident threshold. This application for the AMS ensures all maritime concerns are assessed and security is systematically evaluated nationwide.

Applicability Evaluation For Vessels:

The N-RAT results indicate the following vessel types are at a high risk of a transportation security incident and therefore are required to meet specific security measures as laid out in part 104 of subchapter H:

- All ships, both cargo and passenger, that are subject to SOLAS;
- All vessels greater than 100 gross register tons that are subject to 46 CFR subchapter I (this includes vessels on the Great Lakes);
- All barges subject to 46 CFR subchapter I engaged on an international voyage;
- All domestic passenger vessels subject to 46 CFR subchapters H and K;
- All barges, regardless of route, which are subject to 46 CFR subchapter D and O;
- All tank ships, regardless of route, which are subject to 46 CFR subchapters D and O;
- All Mobile Offshore Drilling Units (MODUs) subject to 46 CFR subchapter I-A;
- All vessels subject to 46 CFR subchapter L;
- All towing vessels greater than 8 meters in registered length that are engaged in towing barges which are subject to 46 CFR subchapter D & O; and
- All towing vessels greater than 8 meters in registered length that are engaged in towing barges that are subject to 46 CFR subchapter I on an international voyage.

The N-RAT results indicate that the following vessel types are at a lower risk of a transportation security incident and are therefore subject to parts 101 through 103 of subchapter H:

- Uninspected vessels, unless otherwise noted;
- Domestic small passenger vessels certificated under 46 CFR subchapter T;
- Barges subject to 46 CFR subchapter I engaged exclusively on domestic voyages;
- Towing vessels engaged in towing 46 CFR subchapter I barges not on international voyages;
- Vessels certificated under 46 CFR subchapter I engaged exclusively on domestic voyages;
- Fleeting tugs or harbor tugs; and
- Other vessels not specifically addressed in part 104 (as an example, recreational vessels).

The inclusion of towing vessels (traditionally included with other uninspected vessels) was done because these vessels interface with and are responsible for the movement of barges that carry higher consequence cargoes, such as Certain Dangerous Cargoes (CDCs). When scored on the N-RAT, the high consequence of the barge cargoes

significantly adds to the risk of a transportation security incident for the towing vessel.

The N-RAT was not able to provide the sensitivity needed to assess certain elements of the definition of a transportation security incident. For example, the transportation security incident calls for a determination of what the term "significant loss of life" should be or where the threshold for an "economic disruption in a particular area" should be placed. In order to determine these elements of a transportation security incident, the Coast Guard used the N-RAT model itself as a guide along with a comparison with other transportation modes. We also used the preliminary intermodal comparison work of the other agencies of the DHS (e.g., TSA).

First, using the N-RAT, we assessed what consequences or combination of consequences would result given a vessel, facility, or port structure that had a high baseline vulnerability. Recalling from the previous N-RAT explanation that the consequence assessment portion of the N-RAT evaluation was based on six categories and five levels (as shown in the table below), we looked at the numerical results of a scenario when given some vulnerability benefits assumed for implemented AMS Plans, and other general security measures in place for a port.

Table 2 Consequence.

Consequence Category / Level	Death/ Injury	Economic Impact	Environmental Impact	National Defense	Symbolic Effect	Follow-on HLS Threat
Catastrophic						
High						
Medium						
Moderate						
Low						

The results showed that a score of at least one consequence factor at the "Catastrophic" level or a combination of two "High" scores could not be offset by the vulnerability reduction achieved by the AMS Plan or general port security efforts. The risk to these types of vessels, facilities, or port structures would need further vulnerability reduction to get out of the potentially "Catastrophic" or "High" consequence arena. This then, is the threshold that the Coast Guard determined could be considered a transportation security incident.

To further determine the thresholds of a transportation security incident with respect to the "loss of life" category, the Coast Guard compared the potential loss for life between various transportation modes and various operations. To look at the "economic disruption"

category of transportation security incident as well as its other elements, we looked at damage and casualty data to determine if comparisons between modes could be used to formulate thresholds based on vessel size.

Passenger Vessel Threshold Determination.

To compare potential loss of life between transportation modes, we examined probable fatalities given an accident to the air, rail, or maritime mode. The first step in this process included a comparison of the current regulatory and operational thresholds that currently exist in each industry.

In aviation, regulations cover aircraft carrying 20 or more passengers as a commuter airline (14 CFR part 125). Most commercial aircraft are larger than this smaller commuter, with 69 percent of the U.S. market dominated by an aircraft with a capacity of 189 passengers.

In rail, we considered transit service (light, heavy, or commuter) and long-haul rail travel. Light rail can carry up to 150 passengers in each car of the train. Heavy rail cars typically carry 100 passengers, though they can carry twice that many during periods of peak traffic. Commuter rail cars carry an average of 125 passengers, with peak capacities of over 200 passengers per car for certain seating configurations. Inter-city rail passenger coaches

typically carry about 80 passengers per car depending on the configuration. The average train length is reported to be 6 to 8 cars.

In the maritime passenger trade, we have small passenger vessels, commuter ferries of all sizes, large passenger vessels, and cruise ships. The average passenger capacity on small passenger vessels is 49. The average capacity for commuter ferries is 587 and for large passenger vessels the average capacity is 1154 passengers.

Looking at casualty statistics for these three modes and different passenger operations, we estimated the probable fatalities given a successful transportation security incident occurred. We assume that, in general, a transportation security incident would have a higher fatality rate than that of an accident because of the hostile motivation behind perpetrators' actions deliberately produce more severe consequences. For aircraft, the more severe airline crashes were used to estimate the transportation security incident fatality rate. The hostile intent may also render certain safety measures less effective in a transportation security incident compared to their demonstrated performance in an accident. We also considered average occupancy rates for each mode into the calculations to estimate a relative

potential loss of life comparison. The table below compares the average estimated fatality rates across modes for various passenger-carrying operations.

Table 3. Comparison of Estimated Fatalities by Mode and Type of Incident.

Mode	Representative Passenger Capacity (Potential Fatalities)	Estimated Average Occupancy (Percent of Capacity)	Estimated Average Occupancy (number of passengers)	Fatality Average Rate*		Estimated Average Fatalities	
				Accident	TSI	Accident	TSI
Air (14 CFR 135) Commuter Plane	80	78%	62	74%	80%	46	50
Air (14 CFR 121) Large Pass. Plane	189	75%	142	74%	80%	105	113
Rail (single commuter car)	180	66%	119	5%	25%	6	30
Rail (6 car commuter Train)	1080	66%	713	5%	25%	36	178
Rail (8 car long-haul Pass. Train)	640	66%	422	5%	25%	21	106
Maritime** (Subchapter H) Large Pass. Vessels (>100 GT)	1154	72%	831	32%	46%	266	382
Maritime** (Ferries – Sub. H & K)	587	72%	423	32%	46%	135	194
Maritime** (Subchapter T) Small Pass. Vessels (<150 pax.)	49	72%	35	32%	46%	11	16

* Accident data from the National Transportation Safety Board and USCG.

** Typical passenger capacity for USCG Documented vessels.

Table 3 shows that per plane/rail-car/vessel, the estimated loss of life from a transportation security incident is estimated to range from a low of 16 per a typical small passenger vessel to a high of 382 for large passenger vessels. The Coast Guard determined that based on the above comparison and the results of the N-RAT vulnerability scores for vessels that result in two "High" consequence scores, that a threshold of 150 passengers is appropriate. We also looked at the N-RAT vulnerability condition for a "Catastrophic" consequence score and determined that added measures were appropriate for vessels carrying 2,000 or more passengers. These additional security measure requirements for larger passenger vessels and the terminals that serve them are justified to offset their elevated risk from a transportation security incident.

Gross Tonnage Threshold Determination.

The N-RAT was also limited in its sensitivity to identify the vessel gross tonnage that sufficiently pointed to a determination of the terms "economic disruption in a particular area, transportation system disruption, or environmental damage" which are required elements of the transportation security incident definition.

Small, dry-cargo vessels (gross tonnage less than 500) were identified by the N-RAT results as vessels of concern. These vessels, regulated under 46 CFR subchapter I and in the gross tonnage range of 15 to 500, are not required to comply with SOLAS and thus are exempt from ISPS Code requirements. We believe this creates a significant security vulnerability that must be considered and addressed at an appropriate level. To establish the appropriate threshold, we evaluated the risk for a transportation security incident posed by smaller vessels (gross tonnage < 500) to determine where a reasonable threshold should be drawn.

The N-RAT results showed a significantly greater risk for vessels of gross tonnage above 100 being involved in a transportation security incident than for smaller vessels. Based on the N-RAT assessment, the smaller vessels (gross tonnage < 100) are unlikely to be involved in a transportation security incident because of the limited consequences they are expected to produce due to their limited size and speed. A review of the domestic freight vessels that are documented with gross tonnage under 100 reveals that less than 2 percent of these vessels are capable of causing significant consequences to facilities or other vessels, and that some of these vessels are

already regulated under this rule due to the nature of the cargo carried. However, because of their greater dimensions and the trades in which they operate, vessels with gross tonnage above the 100 threshold do present the potential of being involved in a transportation security incident. A limited analysis of potential collision effects leads us to the conclusion that these vessels may not be able to cause catastrophic personnel casualties or environmental damage. However, based on our knowledge of port operations, navigable waterways, and vessel design, construction, and operations, we believe that a significant risk of a transportation security incident (one "Catastrophic" or two or more "High" consequence ratings) exists for vessels with gross tonnage above 100. This is primarily driven by potential impact on the economy, national defense, or secondary national security threat from certain scenarios. Examples of these potential effects exist in Coast Guard accident reports where incidents documenting the blockage of channels in various rivers and ports occurred due to vessel casualties. These blockages resulted in substantial economic impacts as the mobility and commerce within the port was seriously affected.

As for the difference in the Convention Measurement tonnage and the Regulatory Measurement tonnage within this analysis, we used the Regulatory Measurement where assigned. There was also an impelling reason to use the Regulatory Measurement for implementing maritime security measures because there is a significant body of existing regulations that are constructed around this measurement system. Therefore, for application, the Regulatory Measurement tonnage (gross register tons) was primarily used unless a certain maritime security requirement was solely meant to reduce risk on vessels that engage in international voyages.

Based on the above, we believe that 100 gross register tons (and not 15 gross register tons) is a reasonable lower end for applicability for dry-cargo vessels. We are also regulating those vessels in the range of 100-500 gross register tons that are not covered by SOLAS and are therefore exempt from ISPS Code requirements.

AIS Threshold Determination.

The applicability thresholds used for the implementation of AIS on certain vessels is a separate issue, for which we did not use the N-RAT. The MTSA clearly mandates AIS applicability in 46 U.S.C. 70114 and the installation dates are included in MTSA sec. 102(e).

The thresholds for vessels: a self-propelled commercial vessel of at least 65 feet in overall length; or a passenger vessel, carrying more than a number of passengers for hire determined by the Secretary; or a towing vessel of more than 26 feet in overall length and 600 horsepower; as well as any other vessel for which the Secretary decides that an AIS is necessary for the safe navigation of the vessel, are related to both safety and security. Thus the thresholds are somewhat lower than those discussed above for vessels at a high risk of a transportation security incident.

Applicability Evaluation for Facilities

The N-RAT results indicate that the following facilities are at a high risk of a transportation security incident and therefore are required to meet specific security measures as laid out in part 105 of subchapter H:

- Facilities that handle cargo subject to 33 CFR part 126, 127, or 154;
- Facilities that receive vessels certified to carry more than 150 passengers;
- Facilities that receive commercial vessels greater than 100 gross register tons on international voyages, including vessels solely navigating the Great Lakes; and

- Fleeting facilities/areas for barges carrying cargoes in bulk, regulated by 46 CFR subchapter D or O or carrying certain dangerous cargoes.

The N-RAT results indicate that the following facility types are at a lower risk of a transportation security incident and are therefore subject to parts 101 through 103 of subchapter H:

- Facilities adjacent to the navigable water that handle/store cargo that is hazardous or a pollutant;
- Facilities that receive only domestic bulk non-hazardous cargo;
- Facilities that service a vessel that carries fewer than 150 passengers;
- Fleeting facilities/areas that service barges subject only to 46 CFR subchapter I or barges that are certified to be gas-free that are certificated under subchapter D and O; and
- Oil and natural gas production, exploration, or development facilities regulated by 33 CFR part 154 that engage solely in the exploration, development, or production of oil and natural gas; and do not meet or exceed the operating conditions in § 106.105 of the

Outer Continental Shelf (OCS) Facilities rulemaking published elsewhere in today's Federal Register;

- Facilities supporting the production, exploration, or development of oil and natural gas regulated by 33 CFR parts 126 or 154 that engage solely in the support of exploration, development, or production of oil and natural gas; and transport or store quantities of hazardous materials that do not meet and exceed those specified in 49 CFR 172.800(b)(1)-(6); or stores less than 42,000 gallons of cargo regulated by 33 CFR part 154;
- Mobile facilities regulated by 33 CFR part 154;
- Isolated facilities that receive materials regulated by 33 CFR parts 126 or 154 by vessels due to the lack of road access to the facilities and do not distribute the material through secondary marine transfers; and
- Other facilities not specifically addressed in part 105.

As mentioned in the above Applicability for Vessels discussion, the 150-passenger threshold will be reviewed for the maritime community when other agencies of DHS (e.g., TSA) have completed their assessment of the national transportation system as a whole and has provided guidance on intermodal thresholds that may refine the "significant

loss of life" determination for the implementation of the MTSA. We are concerned about the gap that may be created by requiring only facilities that service larger passenger vessels to have plans, when some other facilities that service only smaller vessels may, at any point in time, have an aggregation of more than 150 passengers on a facility or pier (such as commuters at small passenger vessel terminals). In addition, small passenger vessels that are not required by subchapter H to have vessel security plans may share the same facility as a larger passenger vessel for which a plan is required. This distinction may put the facility at a higher risk from the small passenger vessel and therefore is a potential "weak link" in the security system. Even though the Vessel Security interim rule found elsewhere in today's Federal Register does not directly regulate these types of small passenger vessels, the facility security plan must nevertheless address the risks presented by accommodating multiple vessel types, even if some of those vessels may not have individual security plans. Additionally, the AMS assessment may indicate that the COTP should impose security requirements on small passenger vessels through the use of orders or security zones to complement those measures being implemented by the facility. The AMS Plan

will reflect what additional necessary measures may be imposed by the COTP on vessels and facilities not subject to parts 104 to 106 of subchapter H, and other activities within the port area, at the three Maritime Security (MARSEC) Levels.

It is important to note the N-RAT focused on the potential for certain vessels and facilities to be involved in a marine-related incident, and its results reflect that relative risk. The Coast Guard took this approach because of our longstanding familiarity with vessel and waterfront facilities, because it was a logical follow-on to the PS-RAT efforts of the COTPs, and because it allowed us to meet the initial mandates of the MTSA to promulgate these interim rules as soon as practicable. However, the MTSA is broader and permits direct regulation of any vessel and facility that may be involved in a transportation security incident, as that term is broadly defined. This could include those facilities and infrastructure not traditionally regulated by the Coast Guard, such as facilities that do not have accommodations for vessels but are nonetheless on or adjacent to waters subject to the jurisdiction of the U.S. The Coast Guard is currently working with other agencies of DHS (e.g., TSA) and other federal agencies to assess the security requirements of

these other vessels and facilities located on or adjacent to waters subject to the jurisdiction of the U.S. Therefore, the interim rules published today, especially the applicability sections of parts 104, 105, and 106, do not exhaust the types of vessels and facilities that may be regulated under the MTSA. We may be involved in follow-on regulations to address these adjacent facilities in the future. In the interim, the AMS Plan will address these types of facilities and COTPs may require specific facilities storing dangerous or pollutant cargoes to add security measures appropriate to their operations and the MARSEC Level.

Applicability Evaluation for Outer Continental Shelf (OCS) Facilities

The N-RAT results indicate that the following OCS facilities are at a high risk of a transportation security incident and are therefore subject to part 106 of subchapter H:

- OCS facilities that produce 100 thousand barrels of oil or 200 million cubic feet of natural gas per day or regularly host more than 150 personnel on a daily basis (may exceed this number for periods of time not in excess of 90 days).

The N-RAT results indicate that the following OCS facilities are at a lower risk of a transportation security incident and are therefore subject to parts 101 through 103 of subchapter H:

- Unmanned platforms and lower production level platforms

The N-RAT was also not able to provide sensitivity to the OCS facility size or production level that sufficiently pointed to a determination of the terms "significant loss of life, economic disruption in a particular area, transportation system disruption, or environmental damage" which are required elements of the transportation security incident definition. To develop this threshold, we worked in conjunction with the Minerals Management Service (MMS) to compare OCS facility production rates and operations throughout the industry. The 150-person threshold was also used to remain consistent with the vessel and facility thresholds. Those OCS facilities that do not fall within the rather narrow parameters of this threshold should consider security measures. We will continue to work with the MMS to validate this threshold as the results of the other agencies of DHS (e.g., TSA) intermodal comparisons are completed. In the interim, the AMS Plan will address these types of OCS facilities and COTPs may require

specific offshore facilities with unique or higher-risk operations to add security measures appropriate to their operations and the MARSEC Level.

Assessment Limitations

While the N-RAT is a very useful tool and offers an excellent way to collect and organize expert judgments about security risk issues, it is not perfect. One limitation is that the quality of the results depends directly on the knowledge and expertise of the expert assessors. Inexperienced personnel with limited perspectives will produce results with limited value. It is essential that seasoned evaluators with a broad experience base be used to ensure full consideration of multiple aspects of the issues. The Coast Guard assessment teams included mid-career and senior professionals with experience in ship design, construction and operation, hazardous materials and facility inspections as well as waterways management and port operations.

Another limitation of the N-RAT is that it looks at risk in a relative way. The N-RAT is considered a "relative risk-indexing" tool, meaning that it is only useful in comparing scenarios evaluated with the tool. The N-RAT does not provide a measure of absolute risk that can be compared to other situations not evaluated in this tool.

A third limitation is that the N-RAT is unable to measure all of the benefits attributable to intelligence or information gathering initiatives, which are commonly called "Maritime Domain Awareness (MDA) initiatives." Measures such as AIS increase awareness and may provide earlier detection or even serve as a deterrent to a transportation security incident, but the assessment tool is unable to capture this effect based on the factors evaluated and the sensitivity of the rating scales. Increased awareness by itself does not decrease the threat or vulnerability at a measurable level subject to the sensitivities of the model. Therefore, the expert panel was unable to account for all of the benefits we believe should be derived from specific MDA initiatives.

Since the N-RAT results highlight the worst-credible case scenarios, a fourth limitation is that the listed results are not sensitive to all scenarios, such as a high profile historically-based incident. We know that small boats loaded with explosives were used as weapons to attack the USS COLE and the tank ship LIMBURG. We cannot discount the possibility of this type of incident in the U.S. or against U.S. vessels outside of the U.S. It is our belief that the best means of deterring such an incident, to the maximum extent practical, is to require certain facilities

used in maritime commerce to conduct an assessment of their vulnerability to being used as a staging area for terrorist activities. These facilities would then construct a detailed plan to control access to the facility, permitting the movement or entrance of only authorized persons and cargoes onto and through the facility. This plan will enable the facility to have increased vigilance, awareness and control over those vessels and persons that are served by the facility. We also believe the possibility of a "COLE-like" incident can be reduced by requiring vessels that would likely be the target of such an attack to likewise assess their vulnerability to such an incident and similarly develop a security plan. This plan would include procedures for security monitoring and increased security vigilance, including security with respect to vessel-to-vessel activities. In addition, vessel and facility plans should include how they would address recreational vessels approaching that they reasonably suspect may pose a threat to them. These facility and vessel security requirements will be complemented by the development of an AMS Plan involving port stakeholders. This plan will address the security measures to be implemented for all port activities at different security levels. The control and movement of vessels, such as small vessels that could be used as a

weapon, will be considered and addressed in the AMS Plan. These controls would include such measures as the possible restriction of all small vessel movements, the implementation and through enforcement of security zones and the coordination of all security patrols in the port.

Lastly, the threat, vulnerability, and consequence scores each have discrete values associated with them. Because there were only 5 scores (1 through 5) for each input variable, the level of resolution (or "granularity") of the risk calculations was limited. This was especially true when assessing the impact of risk reduction initiatives or actions. In many cases, a new initiative or action may have a distinct improvement, but not enough to change a score assignment (e.g., changing the accessibility score from a score of 4 to a score of 3).

Discussion of Comments to Maritime Security Public Meetings

As mentioned, the notice of meeting published on December 30, 2002, requested comments on requirements that align domestic maritime security requirements with the ISPS) Code and recent SOLAS amendments, to comply with section 102 (Port Security) of the MTSA, 2002.

General Comments for all public meetings.

Several comments and issues were discussed at all seven public meetings that reflect general, overarching

concerns of the maritime community for implementing National Maritime Security requirements. These common issues are included in the following discussion.

Commenters voiced the desire to ensure we align the maritime security requirements with other agencies and States that have already tightened security. We have been working with all federal agencies that have security or response related functions and in multiple venues to facilitate the various security initiatives related to homeland security. The joint team that worked on the interim rules found in today's Federal Register is just one example of this type of coordination. Other joint efforts include the ongoing work to implement the Presidential Decision Directive PDD-63 on critical infrastructure protection and The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets. The Department of Homeland Security (e.g., Information Analysis and Infrastructure Protection) is leading this critical infrastructure program. We have also worked with State officials that have implemented maritime security requirements and have broadened this discussion to include all State level homeland security representatives to raise the awareness of maritime security and the importance of the marine elements of the national transportation system

throughout our nation. Further interagency coordination on maritime security issues will also be established when the National Maritime Transportation Advisory Committee is in place. We anticipate that this Committee will assist in ensuring the continued coordination of all involved in maritime security on a national scope.

On a related issue, commenters requested to know how other cargo-handling requirements or proposals by other agencies would affect the maritime industry. Cargo security measures are addressed in 46 U.S.C. 70116, Secure Systems of Transportation, and Section 111, Performance Standards, of the MTSA. Section 111 has an implementation date of January 1, 2004. Other agencies of DHS (e.g., TSA and the Bureau of Customs and Border Protection) are responsible for these sections of the MTSA and will work with the Coast Guard in implementing them. The other agencies of DHS (e.g., TSA and the Bureau of Customs and Border Protection) are actively working toward developing the cargo security measures called for in these sections. They have assembled an interagency team to evaluate the proposals for supply chain security submitted for Operation Safe Commerce (OSC) and hope to have cooperative agreements signed by summer 2003 to analyze supply chain security and

to prototype procedural and technological solutions to supply chain security.

The information gleaned from the OSC effort, as well as information gleaned from other cargo security and productivity initiatives and from experience in other cargo security programs, will form the foundation of forthcoming cargo security regulations. We recognize that, although cargo security will be a component in vessel and facility security plans, facilities and vessels will not want to create and install cargo security technologies in advance of these cargo security requirements, out of a concern that the technologies they create or install will not meet the requirements. Guidelines will be developed and provided for acceptable cargo security measures that can be used until the cargo security requirements are promulgated. These guidelines will address procedural measures.

Again, related to interagency coordination, some commenters stressed the need to harmonize any requirements with the Research and Special Program Administration (RSPA). RSPA published a final rule amending 49 CFR part 172 in the Federal Register on Tuesday, March 25, 2003, (68 FR 14510). The final rule established new requirements to enhance the security of hazardous materials transported in commerce. Like the maritime security interim rules

discussed in this rulemaking, shippers and carriers of certain highly hazardous materials must develop and implement security plans that address three issues: personnel security; unauthorized access; and enroute security. In addition, all shippers and carriers of hazardous materials must assure that their employee training includes security awareness training and, for shippers or carriers of certain highly hazardous materials, in depth employee training for each hazardous material employee. While RSPA's final rule allows training that is conducted and security plans that are prepared to meet regulations, standards, protocols, or guidelines issued by other entities, the final rule comes into effect before the interim rules for maritime security. Shippers and carriers must be in compliance with the RSPA final rule by September 26, 2003. Shippers and carriers that are required to meet the interim rules for maritime security discussed in this rulemaking will have to submit security plans no later than December 2003. As a result, shippers and carriers that must comply with both the RSPA requirements and the maritime security requirements will need to ensure the September date is met. In order to minimize duplicative efforts, we recommend those shippers and carriers develop and implement the training and security plan components of

the maritime security interim rules that also meet the standards of the revised 49 CFR Part 172.800 by September 26, 2003 in order to comply with the RSPA requirements. Because the RSPA regulations do not require plan review, by completing and implementing those portions of the maritime security interim rules that fulfill the RSPA regulations, a shipper or carrier will comply with the RSPA regulations. In other words, if a Vessel or Facility Security Plan is completed and implemented but not yet approved by the Coast Guard, if it contains the elements mandated by the RSPA regulations the shipper or carrier will comply with RSPA. Once the Vessel or Facility Security Plan is approved, both requirements will be met.

Finally, the Environmental Protection Agency (EPA) also has existing regulations for non-transportation-related onshore facilities and certain offshore facilities to prevent the discharge of oil and to prepare plans for responding to discharges of oil or substantial threats of discharges of oil. The Coast Guard and the EPA will continue to explore the impacts of these maritime security interim rules on facilities under EPA jurisdiction and will clarify the impacts of the maritime security regulations, if any, before publishing a final rule. These maritime security interim rules are not intended to require the

owner or operator of a facility under EPA jurisdiction to amend the Facility Response Plan (FRP) or Spill Prevention Control and Countermeasure (SPCC) Plan. We do not intend to require the National Schedule Coordination Committee to modify the existing schedule for exercise. Additionally, we do not intend to require the owner or operator of a facility under EPA jurisdiction to amend the facility's EPA-approved training program, exercises, or drills or record keeping of such training, exercises, or drills. The maritime security regulations for training, exercises, drills, and record keeping in these interim rules are strictly within the purview of the new legislative mandate for security and may be combined with existing training, exercises, or drills, where appropriate.

Commenters requested that we recognize industry-developed standards that achieve an equivalent level of security to the SOLAS and ISPS Code requirements. We have been working on security-related issues and have discussed or required security measures on vessels and facilities (including offshore facilities) since well before the development of the ISPS Code or the MTSA. In this work, we have reviewed and assisted in the development of many industry standards for security that implement high security standards and are effective in preventing

security-related incidents. In addition, we have worked with many States that have successfully developed crime prevention standards for the maritime community that are substantial and effective. Recognizing the substantial body of work in various maritime industry sectors on security, we anticipate recognized industry-developed standards to provide the backbone for implementing many of the security measures contained in the maritime security interim rules found in today's Federal Register. Key to this recognition will be a comprehensive review of the industry-developed standard to determine whether it is equivalent to the security requirements being met by those using the standards found in the maritime security interim rules in today's Federal Register. It is imperative that the industry-developed standards be deemed equivalent in order to ensure that those vessels and facilities that use the industry-developed standards and have a high likelihood of experiencing a transportation security incident have adequately reduced their risk to the benefit of the entire U.S. Marine Transportation System (MTS).

Commenters requested that the requirements be flexible enough to tailor measures to different industries and be performance based rather than prescriptive. Fundamental to the requirements for security has been the concept of a

security assessment. This assessment is specifically linked to security plans and is focused on a vessel, facility, or port as a unique operation. Thus, the assessment results drive the security measures implemented to set or increase each security level and, thus, make each plan unique as well as performance-based. The enforcement of security measures is always difficult when dealing with a purely performance-based system, as opposed to a prescriptive one; however, in this case, it will be clear whether access control, for example, exists or does not. The requirements contained in the maritime security interim rules found in today's Federal Register include clear measures to conduct standard security assessments and draft standard security plans throughout the maritime community. This approach will result in security plans which incorporate specific measures, unique to the operation, but in overall alignment with the objectives of all plans, to detect and deter a transportation security incident.

Commenters requested that the requirements be consistent among ports. We recognized the need for industry to have requirements tailored to their specific and diverse operations yet be afforded the consistency of the larger port-wide security measures. This said, no port has the same critical operations or geographic constraints,

which make mandating the same security measures ineffective. However, we believe the framework of assessments and plans as laid out in the maritime security interim rules found in today's Federal Register, provides the consistency between ports and will be effective. This approach should ensure industry concerns are addressed within each COTP's area of responsibility. Each AMS Plan will also be reviewed and approved at both the District and Area level to assess consistency across the maritime community and to emphasize coordination across all borders. Additionally, we have included some flexibility in the AMS Plan requirements so that some geographic areas can be treated as systems, such as the Western Rivers, the Great Lakes, or the OCS. This geographic coordination of security measures to encompass an entire system will promote effective as well as efficient maritime security for all.

Commenters raised concern on the restrictions to mariner shore leave, detention aboard their vessels, and service provider access to mariners, such as port chaplains, union representatives, etc. This is a very important issue and it is addressed in the Vessel and Facility Security interim rules found elsewhere in today's Federal Register. The interim rules encourage both the

vessel and the facility operators to coordinate shore leave for mariners, as well as procedures for access through the facility by visitors, including port chaplains and union representatives.

Commenters raised concern over the high cost of requirements and disparity between federal funds for the maritime versus the aviation sectors. We understand that many believe the cost of security is overwhelming. The requirements in this set of interim rules focus on those on those vessels and facilities that are at a higher risk of having a transportation security incident. We have developed flexible measures to meet the security requirements. The disparity between funding available between transportation modes is outside the scope of this rulemaking. There are, however, programs, such as the Maritime Security Grant Program, which is funded through the Transportation Security Administration and jointly administered by the Maritime Administration, Coast Guard and the Transportation Security Administration. This grant program can provide some funding for owners and operators regulated under subchapter H. An excellent reference for this program can be found at https://www.portsecuritygrants.dot.tsa.net.

Commenters voiced a desire to have the Transportation Security Card requirements promulgated quickly. As discussed under issue number 37 in the Specific Comments on the 40 issues listed in the public notice section below, there are many credentialing efforts in development. 46 U.S.C. 70105, Transportation Security Cards, addresses unescorted personnel access to secure areas of facilities and vessels. Other agencies of DHS (e.g., TSA) are responsible for implementing this section of the MTSA. Other agencies of DHS (e.g., TSA) are developing the Transportation Worker Identification Credential (TWIC) that will be a transportation system-wide common credential, used across all modes, for all U.S. transportation workers requiring unescorted physical and logical access to secure areas of our transportation system. The goal is to have one standardized credential that is universally recognized and accepted across our transportation system and can be used locally within the current facility infrastructure. We recognize that personnel access control will be a component in vessel and facility security plans, and understanding that facilities and vessels will not want to create and install personnel access control systems in advance of the TWIC infrastructure. In order to address these competing concerns, guidelines will be developed

jointly by other agencies of DHS (e.g., TSA) and the modal administrations, and will provide for acceptable personnel access control measures that can be used until the TWIC is available. These guidelines will address procedural measures.

Commenters requested that we provide guidelines on training requirements for vessel and facility security. The ISPS Code specifies the designation of a Company Security Officer, Ship Security Officer and a Port Facility Security Officer and details their required competencies, duties, and responsibilities. To supplement these requirements, the IMO is developing model courses that identify the key competencies for each of the three security officer positions. The U.S. and India have been asked by the IMO to develop these model courses by September 2003.

In addition to the ongoing international training initiatives, section 109 of the MTSA requires the Secretary of Transportation to develop standards and curricula to allow for the education, training, and certification of maritime security personnel. This task has been delegated to MARAD, which has charged a group of experts at the U.S. Merchant Marine Academy (USMMA) with developing the training requirements for the three security officer

positions as well as the requirements for any other personnel with security duties. The USMMA working group has developed a base-level curriculum for maritime security education. This curriculum was refined through public outreach that included an international conference hosted by MARAD at the USMMA on March 20, 2003.

The "Conference on Maritime Security Standards and Curricula" drew 136 delegates from the U.S. and numerous other countries. The meeting focused on the framework for seven model courses that had been provided to attendees prior to the conference. The seven model course frameworks discussed were:

1. "Vessel Security Officer;"
2. "Company Security Officer;"
3. "Facility Security Officer;"
4. "Maritime Security for Vessel Personnel with Specific Security Duties;"
5. "Maritime Security for Facility Personnel with Specific Security Duties;"
6. "Maritime Security for Military, Security and Law Enforcement Personnel;" and
7. "Maritime Security Awareness."

The discussions also included issues related to certification of personnel and quality control of training

courses. A panel consisting of the USMMA working group members and representatives from the Coast Guard, TSA and MARAD also responded to questions and comments from participants as part of the conference forum.

Ongoing interagency collaboration and efforts to harmonize international and U.S. requirements have led to the expansion of this project to include the development of three model maritime security courses for the IMO. In cooperation with the government of India, the working group prepared and submitted draft model courses for the Ship Security Officer, the Company Security Officer, and the Port Facility Security Officer to the IMO by May 30, 2003. Following review by an IMO validation panel, the finalized courses will be forwarded to the IMO not later than September 8, 2003.

Therefore, the requirements in the vessel security and facility security interim rules found elsewhere in today's Federal Register require the Vessel Security Officer, Company Security Officer and Facility Security Officer positions to have designated personnel and company-certified qualifications until other training provisions are complete. For company-certified qualifications, we anticipate that owners and operators will use the model courses as guidance. Further work on training requirements

and implementation of the security measures may indicate a need to require formal training for these positions, which could be promulgated under a separate rulemaking.

Commenters requested that the process used to determine the applicability of security requirements and their value be explained. We have discussed the initial assessment and subsequent application of these interim rules in the Applicability of National Maritime Security Initiatives discussion above. Additionally we have discussed the value of implementing security measures throughout the maritime community in the Benefit Assessment section of this rule.

Some commenters were concerned about the idea of applying international standards to domestic trade. In the public notice of meeting, we included an appendix that had the ISPS Code and the new security-related SOLAS amendments. We took this approach to provide the public with an opportunity to comment on a body of work that substantially represented the international security requirements and current best practices for maritime security. As stated previously, we had been working on security-related issues and discussed or required security measures on vessels and facilities since well before the development of the ISPS Code or the MTSA. We took these

requirements and discussions further by proposing comprehensive measures for security in our submission to the MSC76 IMO meeting in May 2002. These proposals were developed with respect to security as a system, because fundamental security must be universal — terrorists attack foreign and domestic targets without bias. The flexibility to tailor security plans and measures based on a security assessment is a key to ensuring that a vessel, on either a domestic or non-domestic route, has operational security sufficient to deter, to the maximum extent practical, a transportation security incident. The fact that domestic transportation links are as viable as international avenues for a terrorist attack makes this systems approach even more important, i.e., foreign and domestic vessels must have security measures in place on the same timeframe, making it more difficult to transfer the threat of a transportation security incident to a "softer" target. Finally, the application of ISPS, part B, to all vessels ensures a consistency of security measures implemented while in U.S. ports.

Specific Comments on the 40 Issues Listed in the Public Notice

In the notice, we specifically requested response to 40 issues, helping to shape the regulations published in

all six interim rules. A discussion of the responses to each of the issues raised in the notice follows.

1. Obligations of Contracting Government with Respect to Security. The SOLAS amendments (Regulation 3) and ISPS Code (part A, section 4, and part B, paragraph 4) lay out a series of requirements for Contracting Governments and Administrations to mandate security levels that are appropriate for their vessels and ports. In the notice, we explained our intention to implement these requirements in coordination with the Homeland Security Advisory System (HSAS) and asked for comments on how to relay information to the maritime community on changes in security levels, as well as methods to provide the public a forum to report suspicious acts.

Many commenters viewed as imperative that the threat and security level information be provided quickly and by all means available, including secure web sites or email. They also felt that the information should be provided to all components of the maritime community, including recreational boaters and shore-side personnel, should be formalized, and should be provided proactively. In this interim rule, the process for this communication is formalized through the AMS Plan, which will include all forms of communication available to the COTP in

coordination with the private sector, State, local, and federal agencies. Therefore, a standard communication method will be established across the nation, complemented with regional methods to ensure wide dissemination of threat information and security requirements. As discussed in the Notice for Meeting, the Coast Pilot and Broadcast Notice to mariners will remain key communication tools for vessels underway or coming to the U.S. from foreign ports.

Other commenters suggested that the MARSEC Level should be directly linked to the HSAS at all levels. This contrasts with the comments of many others who voiced a concern about changing levels due to the HSAS system, based on threat information not specifically related to the maritime community nor a specific region. Therefore, they suggested adopting a separate security level mechanism or incorporating some flexibility into the alignment of HSAS to the MARSEC Level. We stated in our notice of meeting that we were considering a link with the HSAS levels and were implementing the MARSEC Level system to ensure both flexibility for the maritime community, as well as to align with the 3-level international security level system. This remains our intent and we have coordinated these alignments with DHS. The regulations lay out further discussion of

the MARSEC Levels and their alignment with HSAS Threat Conditions (see Table 101.205).

Some commenters stressed that coordination with other agencies was needed, and that two-way communications was important to the security of the waterfront and its operations, as is the ability to report incidents that are out of the ordinary. Concern was also noted by some that the communications procedures should directly inform the Facility Security Officers, the Company Security Officers, and the Vessel Security Officers while underway, in lay up, or after hours, since toll-free numbers do not always work from overseas locations or are sometimes reported as busy. We have included other means for communication at the local and national levels in this interim rule to provide alternative means for providing information on suspicious activity. We are working to develop advanced information technologies to interconnect agencies, organizations, vessels, and personnel. The advanced information technologies will facilitate the rapid transmission of critical safety and security information both vertically and horizontally. Additionally, we expect to build a strong communication process with Company Security Officers, Vessel Security Officers, and Facility Security Officers at both the national and area levels once these

Officers are designated and the owner or operator provides their contact information to us.

2. Procedures for Authorizing a Recognized Security Organization (RSO). The ISPS Code (part A, section 4, and part B, paragraph 4) allows Contracting Governments to delegate certain security related duties to a RSO. In order to ensure proper initial implementation of the MTSA and SOLAS, particularly with the accelerated implementation timelines, the Coast Guard discussed in the Notice of Meeting its intent not to delegate authority to an RSO and requested comments on RSO authorities, qualifications, and competencies (other than those listed in the ISPS Code, part B, paragraph 4.5).

Some comments indicated that class societies, while possibly suitable for RSO delegation, should not be considered because of the aggressive timeline to review assessments and plans. Similarly, others indicated their strong support for the Coast Guard to retain all approval authorities, citing that delegation would defeat the purpose and intent of the MTSA. In contrast, some commenters disagreed, stating that the Coast Guard did not have adequate resources. They requested that the Coast Guard delegate its authority to an RSO, establish a timeline for when we would begin consideration of RSOs, and

provide instructions on how RSOs should request consideration. We have retained in this regulation the intent to keep the approval of assessments, plans, and other security measures as a Coast Guard function. While it is understandable that organizations within the maritime community would seek to have their security expertise recognized, the Coast Guard believes it is imperative to maritime and homeland security to ensure consistent application of the requirements found in the interim rules and will conduct the required reviews and approvals without delegation, at this time. A timeline and further delegation discussions may be provided, once a stable, nationwide foundation for maritime security has been established.

As for the adequacy of the list of RSO competencies provided in the ISPS Code, part B, some commenters considered it an adequate list, while others indicated that there should be additional qualifications, such as a familiarity with national and local security plans. We believe this list encompasses the essential qualifications and competencies of organizations that wish to assist the maritime industry in the development of their security assessments and plans. The comment on knowledge of local security plans has merit and should be considered in

addition to the ISPS Code, part B, competencies by those hiring security personnel.

3. Consideration of Other Organizations Competent in Maritime Security. In our Notice of Meeting, we discussed the potential need within the maritime community for assistance with the development of security assessments and plans from organizations advertising maritime security competency. We asked for comments on whether we should establish a standard for these organizations or companies and vet them against a benchmark, such as the one in the ISPS Code, part B, paragraph 4.5.

Several commenters requested that we develop standards or at least an outline of what they should expect from a company that professes maritime security competency and many also stated that the ISPS Code, part B, list was sufficient. Some commenters went further to suggest that we put this standard into guidance rather than regulations or leave it to the trade organizations to develop, because of concern over rigid requirements favoring larger companies and, therefore, limiting the flexibility of owners and operators. Many commenters did not believe the Coast Guard needed to vet these maritime security organizations, however, many suggested that examples of acceptable plans would be helpful to smaller operators. In

contrast, other commenters stated that a list of organizations which meet industry or trade organization standards should be provided, and some went further to recommend the Coast Guard certify organizations, thus creating the basis for a new industry. Finally, some commenters requested that we develop and mandate industry standards for waterborne security and armed guards.

In these interim rules, we reference ISPS Code, part B, paragraph 4.5, as a list of competencies all owners and operators should use to guide their decision on hiring a company to assist with meeting the regulations. We may provide further guidance on competencies for maritime security organizations, as necessary, but do not intend to list organizations, provide standards within the regulations, or certify organizations. We consider standards and requirements for waterborne security and armed guards a subset of the above discussion. While these security measures may be appropriate for some vessels or facilities at a particular MARSEC Level, they are not necessary for all situations. Thus, we have indicated, in only the vessel and facility security interim rules found elsewhere in today's Federal Register, that they are among the additional measures that owners or operators may consider implementing, specifically at heightened security

levels, and COTPs may impose, when deemed necessary to ensure maritime security in certain situations. The standards for private armed security guards are a matter of State and local law, as are the legal parameters for use of force. There are also differing standards that apply to armed private waterborne security in some States and local jurisdictions. Even though the interim rules do not address standards for private security guards in subchapter H, considering this a matter of State and local law and private contract between the owners and operators of vessels and facilities and the security company, we intend to work with State homeland security representatives to encourage the review of all standards related to armed personnel and the services that they provide to the maritime community.

4. Procedures for Accepting Alternatives and Equivalencies. The Notice of Meeting discussed that the SOLAS amendments to Chapter XI-2, Regulation 11 and 12 along with ISPS Code, part B, paragraphs 4.26 and 4.27, allow us to permit alternatives and equivalencies to the security requirements for U.S. flag vessels if they are at least as effective as the mandates and are reported to IMO. This provision is relevant to those vessels operating on international voyages and certificated by the U.S. The

issue of industry standards was raised to cover domestic requirements, and is separate from the alternative and equivalencies provisions in SOLAS. The Coast Guard indicated its intent in the Notice of Meeting to make alternative and equivalency determinations at the national level and requested comment on the provisions of alternatives and equivalencies, as well as the process to submit a proposal to us for consideration (suggesting a process similar to 46 CFR 30.15 or 70.15).

Many commenters suggested that alternatives and equivalency determinations were needed to ensure compliance, yet allow for the unique international operations within some regions or in specific industries. Many commenters also supported the idea of a "master plan" for their vessel fleet or facilities that would eliminate some work and still effectively capture the security measures for the individual vessels or facilities covered. Some also asked if an appeals process would be included so a higher authority could reconsider equivalency and alternative determinations. A few commenters requested that this provision be delegated to the local level rather than be done at Coast Guard Headquarters to account for unique regional operations. Many commenters also stated that the submission process, as it exists for safety (46

CFR 70.15) or subchapter W, is adequate as long as it is timely.

We have included the alternatives and equivalency provisions in this interim rule to provide vessel and facility owners and operators the flexibility to request them. However, they will only be approved if they are determined to be equivalent to the security requirements in subchapter H and 33 CFR parts 120 and 128, if applicable. The provisions of submission and the appeal process are also included in the regulations presented in this interim rule. Because the equivalency and alternative determinations are obligations under SOLAS and the ISPS Code, the Coast Guard is placing the decision to accept equivalents and alternatives at the Commandant level, at this time. This will ensure consistency and retain control over the U.S. flag administration obligation. As always, State, local and regional expertise will be used when reviewing alternatives and equivalencies, as appropriate for the proposals.

5. Procedures for Accepting Industry Standards. In addition to the equivalencies and alternative provisions discussed above, we discussed in the Notice of Meeting that, for those vessels that are currently not required to meet SOLAS, industry standards could be accepted as an

equivalent or alternative. We sought comment on the concept of accepting industry standards and asked whether an independent audit could also be used in conjunction with this system. We also requested comment on the intent to review these standards at the national level and provide a submission process similar to that found at 46 CFR 50.20-30.

An overwhelming number of commenters strongly supported this proposal and voiced endorsements for various industry standards, both for vessels and facilities, which are either published and in use or currently under development. Some commenters recommended that industry standards for assessments already exist that could be determined equivalent to the assessment requirements proposed in the Notice of Meeting and should be considered. Many commenters indicated they intend to submit their standards for approval and will also seek approval for plans or assessments already conducted to meet State requirements. Several commenters also stated that an independent audit should not be required if the vessel is already inspected by the Coast Guard. Many commenters also requested that the industry standards or alternatives be approved at the local or regional level rather than at the Commandant level. Additionally, some commenters expressed

the desire to have the industry standards reflect lower security measures requirements that would not be equivalent to those discussed in the Notice of Meeting.

We have considered the acceptance of industry standards to be a key element of implementing the requirements of the MTSA. The public meeting response to our questions on this issue indicates that the industry is willing to tailor security standards to their industries' needs and work with us to implement them. The issue of equivalency is fundamental to implementing an effective system of maritime security. Therefore, equivalency is a requirement for the acceptance of industry standards in the regulations presented in this interim rule. When a security assessment is conducted on a vessel or facility operation, the resultant security measures that can logically mitigate and meet the security risks are tailored to the situation. Thus, an industry standard for the small passenger industry will be different from the industry standard for chemical ships, simply based on the difference in their respective vulnerabilities and the associated consequence of a transportation security incident. To accommodate this wide diversity of industry standards and substantiate their equivalency to the requirements in subchapter H, the review and approval of industry standards

will remain at the Commandant level. However, we intend to coordinate review of industry proposals with the local and regional levels, if appropriate. In addition, standards already developed to meet State requirements or other industry concerns may be submitted for an equivalency review and subsequently approved under the requirements of this section, if found appropriate. In the requirements of this interim rule, we have titled this industry standard concept, "Alternative Security Programs," because it is a broader term that implies a program or system that is more inclusive, i.e., an industry association or a company could submit these requests for consideration.

6. Declaration of Security (DoS). The ISPS Code (part A, section 5) requires Contracting Governments to determine when a DoS is required for vessels and facilities conducting vessel-to-port or vessel-to-vessel activities. A DoS is a document that establishes an agreement between a vessel and a facility, or between vessels, on their security arrangements to ensure their coordination and communication is clearly set out.

In the notice of meeting, we requested comments addressing recommendations for those operations or security levels when the DoS would be appropriate to facilitate coordination of security measures between a vessel and

facility. As requested, we received comments addressing our question. Comments supported the intent of the requirements but expressed confusion at when it was needed. In particular, ferry operators questioned if they would be required to submit a DoS for every transit. Other commenters suggested that the DoS only be required at higher MARSEC Levels (2 and 3) for specific operations and are not appropriate for domestic vessels. Additionally, commenters suggested that transfers that are brief or involve barges should not have DoS requirements.

We believe a DoS is a valuable security communication tool for vessels, facilities and for COTPs. While a DoS is generally a MARSEC Levels 2 or 3 tool, there are certain operations that benefit from added coordination between the facility and the vessel. In the AMS requirements found elsewhere in today's Federal Register, each AMS Plan will be required to address DoS requirements for certain operations within the ports, especially related to MARSEC Levels 2 and 3. In addition, the AMS Plan will be required to include the procedures for what actions to take when vessels are at a higher MARSEC Level than the Port and request a DoS or other security measures in order to enter the Port. A DoS will not be required for all vessels and all facilities in all operations. In addition to the

requirements found in the AMS Plan, both the Vessel Security and the Facility Security interim rules found elsewhere in today's Federal Register discuss when and for what operations a DoS will be required. We have determined that some operations always require a DoS and therefore vessels engaged in those operations may need to complete a DoS on a regular basis, due to their high-risk operations or locations. However, we believe a standing procedure or agreement can be used to meet this requirement. The COTP may determine, based on the localized repetitive nature of an operation, that a standing agreement which lays out the information in a DoS, can replace the daily use of the DoS.

We also requested comments in our public notice on how long a DoS should be kept on file (we suggested 2-years) and asked how the format of a DoS should be promulgated (guidance or regulation). In addition, the ISPS Code allows flag administrations to give guidance on when their ships should request a DoS during a port call or when interacting with other vessels. Many commenters suggested that 2-year time frame for record retention was much too long. Many commenters also noted that they preferred guidance rather than regulation on the format for a DoS. Based on comments we received and to further align with the ISPS Code requirements, the Vessel Security requirements

found elsewhere in today's Federal Register include requirements to keep DoSs on file for the vessel's last 10 port calls. The Facility Security requirements found elsewhere in today's Federal Register include requirements to keep DoSs on file for the at least 90 days. As for DoS format, the interim rules mentioned above specify required elements for a DoS to ensure facility and vessel forms are acceptable for COTP reviews. For U.S. flag vessels, we intend to provide guidance to Company Security Officers on when to request a DoS based on vessel operations and world threat conditions.

7. Security of Information Contained in Port, Vessel and Facility Security Assessments and Plans. The ISPS Code, part A, sections 9 and 16, and the MTSA (46 U.S.C. section 70101(d)) require documents related to security, especially security assessments and plans, to be kept in a manner that is protected from unauthorized access or disclosure. In our notice of meeting, we asked for comments on whether a classification for sensitive security material would be useful in the implementation of National Maritime Security initiatives.

The majority of commenters supported a designation for all security-related materials to ensure this information is not available to the general public and some requested a

higher security designation such as what the Defense Department is using. Some other commenters did not want a security-related designation because they wished to ensure the Freedom of Information Act remained primary to all information. Other commenters suggested that individuals should have clearances to see this material or that the Coast Guard be the only agency allowed to review the material. In contrast, some State and local government representatives stated their wish to have access to the material and wanted us to include provisions for this access. Additionally, some commenters stated that a federal preemption clause was needed for this designation to ensure that if material was protected from disclosure at the federal level, a loophole at the State or regional level did not compromise its security.

Security-related information has traditionally not been in the public forum since it inherently puts at risk the very system that is being protected. Understanding the imperative need to safeguard maritime security material to ensure its dissemination does not make the vessel, facility, or port vulnerable to a transportation security incident, we have included provisions in this interim rule noting this type of material is to be designated as SSI in accordance with 49 CFR part 1520. Information designated

as SSI is generally exempt under FOIA, and we believe that State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation.

We did not believe that a security designation above SSI was needed for this material however, we did include provisions in this interim rule for a COTP to designate a higher level of security if there are provisions in the AMS Plan that indicate a higher level is appropriate. Access to the AMS Plan will be limited to those on the Area Maritime Security (AMS) Committee that have agreed to protect the material in a manner appropriate to its security sensitivity and have a need to know the material. Guidance on SSI and its use will be issued to assist AMS Committee members, consistent with 49 CFR part 1520. For material that is designated at a level higher than SSI, the COTP will screen AMS Committee members for appropriate clearances and take precautions appropriate to the material's sensitivity. Individuals and Federal agencies outside those with transportation oversight authority will not be allowed to view plans or assessments of vessels and facilities unless circumstances provide a need to view it. As stated in the Vessel Security interim rule found elsewhere in today's Federal Register, certain portions of each vessel security plan and assessment must be made

accessible to authorities; however, those portions not required to be disclosed are protected with the SSI designation and need-to-know criteria. Owners and operators of vessels and facilities may also request a determination of a higher designation than SSI for their plans. The Commandant or the COTP, whoever is responsible for reviewing the security plan, will retain the designation authority. In all cases, the material, if retained by a Federal agency, must be safeguarded to the appropriate designation.

Port Security Provisions.

8. Port Security Plans and Committees. The requirements for port plans stem from the development of the new SOLAS amendments and the ISPS Code as well as the MTSA (46 U.S.C. sections 70103, 70104 and 70112). The definition of port facilities is broad and covers all aspects of the interface between a ship and a facility, including anchorages and other areas typically considered by the U.S. as public waterways, as well as other structures located under, in, on or adjacent to U.S. navigable waters. Thus, in the public meeting notice, we discussed our intention to invoke the alternative provided in ISPS Code, part A, section 16.4, and combine facility plans with a port plan to encompass all waters subject to

the jurisdiction of the U.S. The majority of the SOLAS amendments and ISPS Code requirements would be applied to U.S. facilities to ensure a seamless ship-to-facility security interface. However, the port security requirements will be the overarching instrument for implementing security communications and ensuring compliance. These port requirements will be developed through a port area plan (AMS Plan) and the port security committee (AMS Committee). In our notice, we asked for comments on who should be on the port committee and how we could ensure participation.

The comments we received on the committee's membership included a very broad range of suggestions. Some commenters suggested that only law enforcement entities and relevant government agencies participate. In contrast, many commenters requested that the committee's membership be truly inclusive — representing the smallest of recreational boater, to the largest facility; all types of shore-side service providers, labor representatives, and the myriad government agencies on all levels. Many comments stated the COTP should head the committee and a few comments stated that the COTP and the Port Authority should co-chair the committee.

Commenters suggested that COTPs could ensure participation in the committees by widely disseminating notices about committee meetings, have general public meetings, and hold working meetings to develop security plans. Some commenters recommended a small executive decision-making group with a large inclusive group for input. Some commenters felt there should be Port Security Committees in coastal ports only and voluntary participation with public meetings. Others added that Port Security Committees should be limited to port users and those with security expertise.

Because the AMS Plan is pivotal to the U.S. implementation of the international security requirements and is also key to our MTSA mandates, we have included provisions prescribing the development of AMS Plans, committees, and other port-level security measures in the "Area Maritime Security" (USCG-2003-14733) interim rule found elsewhere in today's Federal Register. This part establishes the AMS Committee, under the direction of the COTP, and indicates that membership to the committee is meant for those with certain skills, port operational knowledge, and should represent all aspects of the maritime community.

9. Port Security Assessments Requirement. In our notice, we also discussed Port Security Assessments (PSAs), as discussed in ISPS Code (part A, section 15, and part B paragraphs 15.1 through 15.16) as well as the MTSA (46 U.S.C. section 70102). Many assessments of this type have already been performed in ports and should be a good foundation for this requirement. Since the assessment will be integral in the development of the AMS Plan, we requested comments on if the committees would be able to provide the experience and expertise needed to do a security assessment and if assessments had already been conducted.

Several commenters stated that they felt that, with the assistance of the local Coast Guard, there would be adequate expertise within the port area to conduct a port wide assessment. In contrast a few commenters stated that the Coast Guard or a third party should conduct the assessments because the knowledge level within the port is not sufficient. Other commenters stated they did not think certain ports even needed to do an assessment because of the port's location. Several commenters also noted that the Coast Guard, both nationally and locally, has already conducted port security assessments.

Our COTPs have been working with Port Security Committees and Harbor Safety Committees successfully for some time. From this positive and participatory interaction, we strongly believe that the knowledge and expertise to successfully accomplish an AMS assessment currently resides in each port, notably within the membership of the current Port Security Committee. We believe that every port needs to conduct a port security assessment regardless of its location. It is important to remember that the current regulations and the international code are intended to strengthen marine elements of the national transportation system as well as lay out a baseline for each section of the system to attain. It is not our intent for ports that have already undertaken security assessments to have to reinvent the wheel rather we encourage AMS Committees to take any assessment that was previously been conducted and use it as a reference document.

10. Port Security Control of Vessels, Facilities, and Operations. The requirements for control of vessels are outlined in the SOLAS amendments, Regulation XI-2/9, and the ISPS Code, part B, paragraphs 4.29 through 4.46. In the notice, we discussed our intention to implement control measures as detailed in the SOLAS amendments and ISPS Code

requirements. However, these measures are not exhaustive and, where appropriate, COTPs will exercise authority under 50 U.S.C. 191, as implemented at 33 CFR part 6, 33 U.S.C. 1226, 33 CFR parts 160 and 165, and other measures consistent with international law, to ensure maritime security. In addition, we outlined our intent to ask the Port Security Committee (AMS Committee) to review areas within the port, such as fleeting areas, regulated navigation areas, anchorages, and areas near facilities, to assess whether these areas should have security zones or patrol requirements established at certain security levels. We asked for comments on the concept of a set of security zones or requirements set out in this pre-designated fashion with a specific procedure for triggering its implementation through a broadcast notice to mariners or security level communication to the maritime community. We asked if such a pre-designation would assist mariners and if other possible control measures would be recommended.

Many commenters supported the concept of a pre-designated system of waterway and facility restrictions and stated it would be advantageous for planning and preparation. They continued by suggesting that at times of heightened security, we should use existing maritime communications procedures as well as any other means to

ensure vessels are advised to hold, or move to designated anchorage outside of port. Other commenters wanted to ensure that the barge and towing industry was consulted on any decisions to restrict the waterway. Some commenters stressed that communication methods of these pre-designations should include the entire maritime community such as recreational boaters and shore-side interests. A few commenters also suggested that other control measures would include setting barriers and booms to deter seaward access.

As stated previously, the AMS Plan and the supporting committee is an integral part of the port security initiative. Measures that mitigate security risks to the port for each security level will be a main element of the AMS Plan as discussed in the "Area Maritime Security" (USCG-2003-14733) interim rule found elsewhere in today's Federal Register. We have outlined in these requirements a broad range of communication methods intended to include all sections of the port community and requirements for the AMS Committee to evaluate all options available to restrict or control activities in each port at each MARSEC Level. However, the COTP may independently exercise his or her broad statutory and regulatory authority to implement any measures deemed necessary to ensure maritime security.

11. Port Security Training and Exercises. In the notice, we explained that ISPS Code (part A, section 18 and part B, paragraphs 18.1 through 18.6) detail training, drills, and exercise requirements for port facilities. We requested comments on whether the maritime community would participate in port-level security exercises and what type of exercise is most desirable. We also asked for comments on existing port security training programs. Most commenters stated that while they would participate in port-level security exercises, a 12 to 18 months frequency was preferred. They also suggested that the COTP should vary drill schedules to reflect local conditions/threats. Commenters also suggested that only small portions of the Security Plan be exercised at a time and recommended that communications be tested more frequently than other sections of the plan. Some commenters stressed that combining security exercises with port pollution/disaster exercise is preferable, and that tabletop exercises or seminars should be considered in lieu of a full exercise. A few commenters stated that industry already trains security personnel and others commented that there should be no requirements for training. Other commenters recommended self-certified security training at the port-

level and some believed Coast Guard auxiliaries need security training.

We believe that exercises and training are imperative to keeping security measures and plan requirements current. To ensure that the entire port community participates, we want to establish exercise programs that are inclusive and training that is exportable. In the "Area Maritime Security" (USCG-2003-14733) interim rule found elsewhere in today's Federal Register, requirements for exercises and drills are included. To add flexibility, provisions have been made to credit tabletop exercises as well as full deployment exercises. We anticipate that security will be a part of all port-level exercises such as pollution response or rescue drills. In addition, due to the nature of most ports, high-profile public events such as marine parades or festivals will likely mean an actual exercise of the ATMS plan that meets the intent of the exercise requirements. While these high-profile public events would require a marine event permit, we will not require that marine event permits be obtained for port-level training exercises. Training requirements for port personnel have not been included in the interim rule. It should be noted however, that the MARAD is developing education and training guidelines for maritime security professionals,

some of which are intended for port security personnel. We intend to evaluate these guidelines when developed, and determine at that time whether further requirements are needed to ensure the competency of security personnel at the port-level.

Vessel Security Provisions.

12. Incorporation by Reference. In the notice of public meeting, we discussed the concept of accepting national, State, and industry security standards to meet certain security requirement(s), such as a vessel security plan that incorporates the use of motion detection equipment that meets an accepted national standard. We requested that commenters share known national, State, or industry standards that could be used as an equivalent to our requirements in the marine environment and we asked them if they would use such standards, if available.

Many commenters supported our concept noting the flexibility of using existing standards, such as the ones prepared by the intrusion detection and surveillance industries. A few commenters stated that while they supported using existing standards, they were concerned about conflicts and incompatibility between current security equipment and equipment used for shipboard operations, while several others approved of the

flexibility of using equivalent standards and stated that as long as we approved the use of the standard they would submit it as an equivalent standard to the requirements. Other commenters stated that they were against the use of industry standards and feared the Coast Guard would micro-manage vessel security operations.

Traditionally we incorporate by reference equipment standards we feel are appropriate to use in the maritime environment to enable vessel and facility owners and operators the flexibility to use standards they are familiar with as well as ones that are appropriate to meet the requirements. In the maritime security regulations for subchapter H found in today's Federal Register, there are no national, State, or industry equipment standards incorporated by reference because specific standards were not identified. However, a section in this interim rule (part 101) has been reserved for listing equipment standards for incorporation, if found appropriate in the future.

13. Obligations of the Company. In the public notice we discussed the concepts in SOLAS amendments (Regulation 4 and 5) and the ISPS Code (part A, section 6, and part B, paragraphs 6.1 through 6.8) that obligate the company for certain requirements. We requested comments on these

obligations and whether they were sufficient to address maritime security. We also asked for comments on how to treat the special relationship between towing companies and barges.

Many commenters felt that this provision would clarify the companies' responsibility to the vessel and address any potential manning issues, while a few comments stated that the requirements for a company were "excessive" or that the ISPS Code did not address the requirements needed. Many comments stated that an independent audit of the Vessel Security Plan would be valuable in determining if the company's obligations and responsibilities were addressed and properly implemented.

In regards to the relationship between tows and barges, a large number of comments stated that the towing vessel should be responsible for the security of the barge while it is under their control. Several other comments recommended that security at fleeting areas be regulated.

We support holding the company to security-related obligations that will ensure companies and the vessels communicate on issues related to security, and help to ensure that any problems are resolved in an efficient manner. We believe proper implementation cannot work without the company and the vessel fulfilling their

obligations as stated in the ISPS code. The company is essential to ensuring that the right people with the right skills are in the Company Security Officer, and Vessel Security Officer positions. A company will not need to establish new internal guidance to satisfy the requirements if it already has guidance in another document that meets the requirements of the ISPS Code.

We reviewed the concept of an independent audit and have addressed it in the Vessel Security interim rule found in today's Federal Register. The unique relationship between a towing vessel and its tow has been considered and requirements for both are included in the vessel security requirements found elsewhere in today's Federal Register. Fleeting areas are also addressed in the Facility Security interim rule found in today's Federal Register.

14. Vessel Security Requirements. In the public notice we discussed that the SOLAS amendments (Regulation 4) and the ISPS Code, part A, section 7, require vessels act upon security levels set by Contracting Governments through appropriate protective measures by carrying out certain specified activities (ISPS Code, part A, section 7.2). We also asked whether the security measures should apply to other vessels that were not listed in the notice

and whether these activities and protective measures adequately address the security of a vessel.

A very large number of commenters addressed the issue of which vessels the regulations should be applicable to. This issue has been discussed in the General Information section above, under the subheading Applicability of National Maritime Security Initiatives.

Several commenters noted possible alternative measures to be used in meeting the requirements, which are not specifically listed in the ISPS Code. The requirements in this general interim rule give provisions for both vessels and facilities to use Alternative Security Programs to meet the requirements. We will continue to provide feedback to industry, via Internet webpage and public notice, on all Alternative Security Programs that are approved by the Coast Guard (G-MP) as alternatives.

15. Vessel Security Assessments (VSA) Requirement. In the notice we discussed the requirements for a Vessel Security Assessment contained in the ISPS Code and the MTSA. We also discussed our desire to have a Vessel Security Assessment for each vessel that has to develop a security plan. In the notice of public meeting we asked for recommendations on how to conduct a Vessel Security Assessment for a vessel on a domestic voyage, and whether

we should consider any existing alternatives to a Vessel Security Assessment.

Commenters recommended that we allow industry produced assessment tools, or require all assessments to be conducted by an objective third party, while others requested that we develop a template to be used in a self-assessment process. A few commenters claimed that a security assessment had already been done by the Coast Guard and requested that it be used in place of the required Vessel Security Assessment to avoid duplication of effort.

We strongly support the use of third-party assessments and audits to ensure quality as well as consistency. However, we are not including this provision as a mandatory requirement in the Vessel Security interim rule found elsewhere in today's Federal Register because the assessment is one part of the vessel security plan that we will be closely reviewing prior to the plan approval. We are assisting in the development of several assessment tools and templates. We recommend that vessel owners and operators seek tools from appropriate industry sectors that support or represent them to aid in completing the security assessments. To reduce the duplication of effort, we also strongly encourage vessel owners and operators to use any

information that was previously collected during a security assessment as reference material for completion of the applicable areas of the new assessment.

16. Vessel Security Plan Requirement. In the public notice we discussed the development of a Vessel Security Plan that takes into consideration a Vessel Security Assessment, and makes provisions for actions at each of the three MARSEC Levels. In the notice we referenced the vessel security plan requirements in the ISPS Code and asked for suggestions about additional items or best practices to be addressed by the Vessel Security Plan. We also inquired whether an outline would aid you in developing a vessel security plan.

We did not receive comments suggesting additional items be addressed in the Vessel Security Plan, but we did receive multiple industry and organization submissions of their standards for consideration as a vessel security plan best practice. Many commenters stated that allowing an existing industry standard to be used would greatly streamline the review process. A number of others asked if we could provide a "model plan" for them to use. Many commenters also requested the acceptance of fleet-wide plans. Several owners also asked if a vessel and a facility, which have an exclusive docking arrangement (one

in which no other vessels dock at the facility and the vessel only docks at the facility pier), could submit a uniform vessel/facility security plan.

The strong response and industry standards submitted as examples of best practices lead us to believe that the maritime industry is implementing security measures in many sectors. Many of these industry standards did have "model plans" incorporated into them as a development aid. As discussed previously, we will allow organizations to submit their security programs for consideration as an alternative to the requirements in the vessel security interim rule found elsewhere in today's Federal Register. The concept of accepting fleet-wide plans or plans that discuss exclusive docking arrangements or a single plan to cover both a terminal and a vessel, could also be considered Alternative Security Programs and be accepted if they meet the specified requirements.

17. Submission of Vessel Security Plans for Approval. The public notice discussed the need for a vessel to carry on board an approved Vessel Security Plan. In the notice of meeting, we requested suggestions on how vessel security plan approvals could be streamlined. We also asked if the format we proposed was appropriate or if an alternative process existed that we should consider.

Several commenters questioned the consistency of Vessel Security Plans approved by varying COTPs and asked what safeguards would be in place to ensure consistent enforcement for vessels that operate across COTP boundaries. In contrast, many other commenters felt the approval at the local COTP level would ease the process and allow for someone familiar with the vessel's operations to review the Vessel Security Plan. Finally, some commenters were also curious about the procedure for reviewing foreign vessel security plans.

To ensure a consistent approval process, we have decided that the Marine Safety Center (MSC) will review and approve all vessel security plans. This requirement is included in the Vessel Security interim rule, found in today's Federal Register. For those Vessel Security Plans with specific local or regional considerations, we will ensure that the local COTP or District personnel will be able to interject any industry or geographic specific information into the approval process.

It is not our intent to individually approve vessel security plans for foreign SOLAS vessels coming to the U.S. Consistent with our international obligations under SOLAS and the ISPS Code, we will deem flag administration approval of a ship security plan to constitute approval

under 46 U.S.C. 70103, provided the ship security plan complies with SOLAS and ISPS Code, part A, having fully applied the relevant provisions of ISPS Code, part B. Compliance by foreign SOLAS vessels will be addressed under the Port State Control program, with plans being reviewed by the vessel's flag administration as required by SOLAS and the ISPS Code.

However, in certain cases, foreign vessel operators may be required to submit the vessel security plan to the U.S. for approval, as required in the Vessel Security interim rule found elsewhere in today's Federal Register. These foreign vessels are an exception because they fall outside of the tonnage or route thresholds for SOLAS obligations, yet trade with us and, for security consistency, should meet the same security requirements as those vessels covered under domestic law.

18. Existing Security Measures for Certain Vessels. As mentioned in the notice of meeting, we are evaluating the need for retaining existing security requirements that are contained in 33 CFR part 120, for certain vessels (e.g., large passenger vessels) that could be involved in a transportation security incident. More specifically, the notice asked whether additional security requirements are needed for certain vessel types.

Many commenters noted that the standards of the ISPS Code provided more than adequate security measures and could be considered equivalent to the existing 33 CFR 120 requirements.

Because we are still evaluating the equivalency of 33 CFR 120 to the requirements in the Vessel Security interim rule found elsewhere in today's Federal Register, we do not intend to revise 33 CFR 120 at this time. However, in the future, this part may be revised or entirely deleted. This will consolidate the security requirements for all vessels in subchapter H.

19. Vessel Security Recordkeeping. In the notice of meeting, we requested suggestions or best practices related to recordkeeping. We also asked whether we should prescribe a format for these records.

Numerous commenters asked that industry standards be accepted for recordkeeping and that companies and vessels be allowed to decide where to keep records. Several commenters questioned the need to keep records for two years, while others stated that there was no need to keep records. Several commenters asked that a format not be specified but that the Coast Guard provide clear guidance on what type of information should be kept.

We believe that industries have developed suitable internal guidance for keeping records. These records are essential to ensuring compliance and for this reason we are requiring security records be maintained for two years. Specific guidance on what type of information must be kept is included in the Vessel Security interim rule found in today's Federal Register, with flexibility to choose their format and where the records are kept.

20. Company Security Officer Designation. In the notice of public meeting, we asked whether Company Security Officers should be required to attend training and if company certification is appropriate to verify the Company Security Officer's qualifications. We also acknowledged that many companies already have training programs in place.

Several commenters stated that it was reasonable for the company to train and certificate the Company Security Officer, while other commenters believed it was a conflict of interest. Others commented on whether records should even be kept; some stated that no records should be kept and some recommended that the records should be kept for a period of one to three years.

We recognize there are no approved courses for the Company Security Officer at this time. In the absence of

approved formal training, we intend to allow companies to certify that personnel holding the Company Security Officer position have received appropriate training or possess the job experience required to fulfill their Company Security Officer duties, based on the requirements in the Vessel Security interim rule found in today's Federal Register.

We believe that the Company Security Officer's participation in exercises is critical to improving security. In order to ensure the Company Security Officer has participated in appropriate port-level exercises, we are requiring records, including a list of participants, to be kept for 2 years.

In addition to the questions we asked in the notice of meeting, we received several comments outside of those questions regarding the Company Security Officer. Several commenters expressed confusion about the requirements for a Company Security Officer. To clarify, a company with a large fleet may decide to group its vessels and assign a Company Security Officer to each group. This company would then have several Company Security Officers, one Company Security Officer per vessel group. While the Company Security Officers are responsible for the security of the vessels in their group, they may not act as Vessel Security

Officer, except as exempted by the requirements in Vessel Security interim rule found in today's Federal Register.

21. Vessel Security Officer Designation. In the notice of public meeting, we asked whether Vessel Security Officers should be required to attend training and if company certification is appropriate to verify the Vessel Security Officer's qualifications. We also acknowledged that many companies already have training programs in place.

Numerous commenters supported allowing company certification and felt formalized training was a good system to certificate personnel. A small group of commenters saw no need for any formalized training or company certification. We did not receive any comments to our request for suggestions for certain classes of vessels being allowed an alternative to a Vessel Security Officer.

We recognize that Vessel Security Officer security training is not currently formalized, however, it would be beneficial as previously discussed in the Discussion of Comments to Maritime Security Public Meetings section of this preamble. In the absence of approved formal training, we intend to allow companies to certify that personnel holding the Vessel Security Officer position have received appropriate training or possess the job experience required

to fulfill their Vessel Security Officer duties, based on the requirements in the Vessel Security interim rule found in today's Federal Register. Although we did not receive any suggestions on alternatives to a Vessel Security Officer, provisions within the Vessel Security requirements found elsewhere in today's Federal Register, do not preclude a Company Security Officer from also acting as a Vessel Security Officer.

22. Security Training and Drill Requirements for Vessel Personnel. In the notice of public meeting we requested comments on whether we should require vessel security personnel to attend formal training. We discussed the concept of allowing the company, and its Company Security Officer, Vessel Security Officer, Facility Security Officer, or Vessel Master to certificate security officers and train the vessel personnel in accordance with the requirements. We also asked if prescribing the format for training records would assist the companies.

Several commenters agreed that the company and its Company Security Officer, Vessel Security Officer, Facility Security Officer or Vessel Master should certificate security officers and train the vessel personnel, while a few commenters saw no need for formalized training. A few commenters also stated that the drill and exercise

requirements were excessive. Several commenters recommended we provide specific requirements on the type of information that should be recorded, but not require a specific format for record keeping.

As previously stated, there are no approved courses for vessel personnel. In the absence of approved formal training, we intend to allow companies, Vessel Masters, Vessel Security Officers, Facility Security Officers, or Company Security Officers to certify that personnel holding a security position have received the training required to fulfill their security duties.

When training is developed, we will reassess the training and certification requirements in the Vessel Security interim rule found in today's Federal Register. We will then propose alternatives or additional requirements in a separate rulemaking, as appropriate.

We have included the specific requirements in the Vessel Security interim rule, found in today's Federal Register, on what type of information must be kept, with the vessel owner or operator deciding what format and where the records will be kept.

We believe it is imperative that exercises and drills be conducted to ensure the plans are current and that the personnel are familiar with their responsibilities.

Therefore, we have included exercise and drill requirements in the Vessel Security interim rule found in today's Federal Register. Security drills and exercises can be incorporated into existing response exercises and drills and we believe that by combining exercises, when possible, the exercises and drilling requirements can be made more efficient.

23. Certification for Vessels. In the notice of public meeting we discussed the certification requirements for an ISSC and requested suggestions for how best to verify and certificate compliance.

Many commenters suggested that amending a vessel's Certificate of Inspection or a letter stating compliance with security requirements would be adequate. Other commenters recommended allowing third-party certification rather than Coast Guard certification.

We believe certification and verification can be accomplished during a regular Coast Guard Inspection and the vessel's certificate can adequately reflect compliance. In addition, for those uninspected vessels requiring security measures, other provisions for documentation are provided in the Vessel Security interim rule, found elsewhere in today's Federal Register. We have not included provisions for third-party certification, however

we have included provisions for Alternative Security Programs that could streamline the certification process.

Facility Security Provisions

24. Incorporation by Reference. In the notice of public meeting, we stated we were considering accepting national, State, and industry security standards to meet certain security requirement(s), such as a facility security plan that incorporates lighting or fencing equipment that meet an accepted national standard. We requested that commenters share known national, State, or industry standards that could be used as an equivalent to our requirements in the marine environment and we asked them if they would use such standards, if available.

Many commenters supported our position of including a provision for accepting national, State, and industry security standards as an equivalent to meet certain security requirements. Several commenters confirmed that those within the security industry, such as the fence and lighting industries, should be allowed to continue providing their own security standards and that in general, companies would meet marine industry-wide standards once the Coast Guard approved them. Finally, many commenters expressed concern that if the Coast Guard prescribed

measures to be used as industry standards that the measures would be in excess of what is needed.

Traditionally, we incorporate by reference equipment standards we feel are appropriate to use in the maritime environment to enable vessel and facility owners and operators the flexibility to use standards they are familiar with as well as ones that are appropriate to meet the requirements. In the maritime security regulations for subchapter H found in today's Federal Register, there is no national, State, or industry equipment standards incorporated by reference because specific standards were not identified. However, a section in this interim rule (part 101) has been reserved for listing equipment standards for incorporation, if found appropriate in the future.

25. Facility Security Requirement. In the public notice, we discussed that the SOLAS amendments (chapter XI-2, regulation 10) and the Code (part A and part B, section 14) require facilities to act upon security levels set by Contracting Governments through appropriate protective measures by carrying out certain specified activities (ISPS Code, part A, section 14.2). We also asked whether the security measures should apply to other facilities that were not listed in the notice and whether current

activities and protective measures adequately address the security of a facility.

A large number of commenters addressed the issue of which facilities the regulations should be applicable to. This issue has been discussed in the Applicability of National Maritime Security Initiatives section above.

We did not receive any comments specifically addressing the request for suggestions on additional requirements that could be used.

Several commenters stated that barge fleeting areas should be covered under the new requirements. To address fleeting areas and the security of the barges that use them we have included fleeting areas in the Facility Security interim rule found in today's Federal Register.

26. Facility Security Assessments Requirement. In the notice, we discussed the requirements for a facility security assessment contained in the ISPS code and the MTSA. We also discussed our desire to have a facility security assessment for each facility that has to develop a facility security plan. In addition, we asked if there were any recommendations on how to conduct a facility security assessment and if any appropriate alternatives to a facility security assessment already existed that we should consider.

Several commenters stated that they have used NVIC 11-02 titled, "Security Guidelines for Facilities" or similar approaches in developing a company assessment plan and found them easy to follow. Other commenters offered alternatives, such as a Coast Guard facility inspection or a Navy facility security assessment.

We have included requirements for facility assessments in the Facility Security interim rule found elsewhere in today's Federal Register. In addition we have been assisting in the development of several industry and Federal assessment tools and templates. We are aware that other agencies of DHS (e.g., TSA) are developing a self-assessment tool. We understand that they intend to mandate use of this tool in the future. We recommend that facility owners and operators seek tools from appropriate industry sectors that support or represent them to aid in completing the security assessments. To reduce the duplication of effort, we also strongly encourage facility owners and operators to use any information that was previously collected during a security assessment as reference material for completion of the applicable areas within the new assessment. There are also provisions in this interim rule for the use of alternative assessment tools however; tools such as the Department of Defense assessment have not

been specified because we have focused on the specific needs required for transportation-related assessments.

27. Facility Security Plans Requirements. In the public notice, we discussed the ISPS Code (part A and part B, section 16) as well as the MTSA (46 U.S.C. sections 70103 and 70104) that takes into consideration a facility security assessment, and makes provisions for actions at each of the three MARSEC Levels. We also asked for suggestions about additional items or best practices to be addressed within the facility security plan requirements.

We did not receive any comments specifically addressing additional items that the facility security plan should cover, however, many commenters did state that an outline would be a useful tool for development. Several of these commenters went on to say that a "model plan" would prove to be a better guide because it would clearly show our expectations of a plan. Several commenters noted that there are companies that own many facilities and vessels, and asked if one combined security plan could be submitted to avoid redundancies in submissions.

The strong response and industry standards submitted as examples of best practices lead us to believe that the maritime community is implementing security measures in many sectors. Many of these industry standards did have

"model plans" incorporated into them as a development aid. As discussed previously, we will allow organizations to submit their security programs for consideration as an alternative to the requirements in Facility Security interim rule found elsewhere in today's Federal Register. The concept of accepting fleet-wide plans or plans that discuss exclusive docking arrangements, or a single plan to cover both a terminal and a vessel, could also be considered Alternative Security Programs and be accepted if they meet the specified requirements.

28. Submission of Facility Security Plans for Approval. In the public notice we discussed the ISPS Code, part A, section 16, requiring facilities to develop and maintain a facility security plan that is approved by the Contracting Government in whose territory the facility is located. We asked for suggestions on how facility security plan approvals could be streamlined. We also asked if the format we proposed was appropriate or if an alternative process existed that we should consider.

There was large support for the local COTP to approve facility security plans. Some commenters asked how the Coast Guard would ensure consistency across COTP zones. Several commenters approved of the format Coast Guard presented, but did not want a mandated format.

As stated in the notice of meeting, we intend for the COTP to approve facility security plans and we will also work to ensure there is consistency between COTP zones. The Facility Security interim rule found elsewhere in today's Federal Register contains an outline to be followed when constructing a facility security plan. This outline format provides facilities with leeway during the development process of their facility security plan. Contracting Governments to SOLAS will approve the security plans for port facilities within their territory. These Contracting Governments are also responsible for notifying the IMO regarding which port facilities within their territory have approved security plans. As discussed previously, a vessel calling on a foreign port facility that does not comply with SOLAS and the ISPS Code or at a port that does not maintain effective anti-terrorism measures, will be subject to scrutiny under our Port State Control Program to ensure that the security intended to be achieved by this subchapter will not be compromised.

29. Facility Security Recordkeeping. In the notice of meeting, we requested suggestions or best practices related to recordkeeping. We also asked whether we should prescribe a format for these records.

Many commenters supported our position on keeping records for two years, while others questioned it and some opposed the concept of maintaining these records at all. Numerous commenters asked that industry standards be accepted or that companies and facilities be allowed to decide where to keep records. Several commenters requested specific guidance on the type of information that should be kept, but did want the format not be specified. Some commenters proposed that third parties be required for record keeping.

We believe that industries have developed suitable internal guidance for keeping records. These records essential to ensuring compliance and for this reason we are requiring security records be maintained for two years. Specific guidance on what type of information must be kept is included in the Facility Security interim rule found in today's Federal Register, with flexibility to choose their format and where the records are kept. Finally, we feel requiring a third party to keep all records would cause undue burden to the facilities.

30. Facility Security Officer. In the notice of public meeting, we asked whether Facility Security Officers should be required to attend training and if company certification is appropriate to verify the Facility

Security Officer's qualifications. We acknowledged that many companies already have training programs in place. We also asked if Facility Security Officers might be performing their duties for more than one facility.

The majority of the commenters stated that companies should be allowed to verify qualifications and certificate Facility Security Officers. A few commenters felt it was a conflict of interest for the company to certificate a Facility Security Officer as meeting the knowledge level. We also received many comments about required formal training; some of the comments were in favor and some felt it was not necessary. Several commenters submitted examples of cases where the Facility Security Officer could be responsible for more than one facility. Finally, many commenters stated that the record keeping requirements were reasonable and could be easily instituted, while others stated this task would be too time consuming.

We recognize that Facility Security Officer security training is not currently formalized, however, it would be beneficial as previously discussed in the Discussion of Comments to Maritime Security Public Meetings section of this preamble. In the absence of approved formal training, we intend to allow companies to certify that personnel holding the Facility Security Officer position have

received appropriate training or possess the job experience required to fulfill their Facility Security Officer duties, based on the requirements in the Facility Security interim rule found in today's Federal Register. We do not see this authority as a conflict of interest.

We agree that a Facility Security Officer could oversee the security operations at more than one facility, where facility security plans are very similar because of similar operations and in close proximity of each other. This decision will be left to the local COTP when plans are being approved.

31. Security Training, Drills and Exercises for Facility Personnel. In the notice of public meeting we requested comments on whether we should require facility security personnel to attend formal training. We discussed the concept of allowing the Facility Security Officer to certificate security officers and train the facility personnel in accordance with the requirements. We also asked if prescribing the format for training records would assist the companies.

Several commenters recommended that we provide specific guidance on the type of information that should be recorded, but not require a specific format for the

recordkeeping. Other commenters stated that the drill and exercise requirements were excessive.

As previously stated, there are no approved courses for facility personnel. In the absence of approved formal training, we intend to allow Facility Security Officers to certify that personnel holding a security position have received the training required to fulfill their security duties.

When training is developed, we will reassess the training and certification requirements in the Facility Security interim rule found in today's Federal Register. We will then propose alternatives or additional requirements in a separate rulemaking, as appropriate.

We have included the specific requirements in the Facility Security interim rule, found in today's Federal Register, on what type of information must be kept, with the facility owner or operator deciding what format and where the records will be kept.

We believe it is imperative that exercises and drills be conducted to ensure security plans are current and that the personnel are familiar with their responsibilities. We also believe that the Facility Security Officer's participation in exercises is critical to improving security. Therefore, we have included exercise and drill

requirements in the Facility Security interim rule found in today's Federal Register. Security drills and exercises can be incorporated into existing response exercises and drills and we believe that by combining exercises, when possible, the exercises and drilling requirements can be made more efficient.

32. Certification for Facilities. In the notice of meeting, we requested suggestions for verification and certification that facilities do comply with the security regulations. We also asked whether we should allow companies to certify their facilities.

A large number of commenters stated that self-certification which reflects a current industry standard and has an independent audit would be appropriate. Other commenters supported the role of the Coast Guard in oversight during the certification process.

We intend to approve all facility security plans and compliance with the requirements in the Facility Security Interim rule found in today's Federal Register. We believe certification and verification can be accomplished during a Coast Guard Inspection and the facility's plan approval letter sufficiently documents compliance when viewed in conjunction with other security-related records. We have not included provisions for third-party certification in

the Facility Security interim rule, found in today's Federal Register however we have included provisions for Alternative Security Programs that could streamline the certification process.

Other Security Provisions.

33. Permanent Hull Marking Requirement. In our notice of meeting, we discussed the SOLAS amendments creating a new regulation in Chapter XI-1 (Regulation 3) that requires vessels to have their identification number permanently marked on their hull and in an easily accessible place on the transverse bulkhead of the machinery space or on another suitable interior location, as specified. We discussed our intention not to extend the application of this requirement to vessels limited to domestic voyages and requested comments on this SOLAS provision and its application to the domestic trade.

An extremely large number of comments were received on this issue. Almost every comment strongly supported our concept to not require the hull markings for vessels that only engage in domestic voyages, including all international voyages not subject to SOLAS. Several commenters asked for exemptions for certain vessel types such as historically significant vessels. We believe that the requirement should not be extended to domestic vessels

and, in the Vessel Security requirements found elsewhere in today's Federal Register, we have only applied the requirement to those vessels obligated to meet the SOLAS requirement. In accordance with SOLAS, a passenger vessel of 100 gross tonnage, ITC and upwards, and cargo vessels of 300 gross tonnage, ITC and upwards, on an international SOLAS voyage should be marked in accordance with its guidance.

34. Continuous Synopsis Record Requirement. In our notice of meeting, we discussed the SOLAS amendments that created a new regulation in Chapter XI-1 (regulation 5) that requires vessels to maintain and update a Continuous Synopsis Record, to be kept on board, that contains information such as the name of the flag administration, the date of the vessel's registry, the vessel's identification number, etc. We discussed our intention not to extend the application of this requirement to vessels limited to domestic voyages and requested comments on this SOLAS provision and its application to the domestic trade.

An extremely large number of comments were received on this issue. Almost every comment strongly supported the Coast Guard position of not requiring the Continuous Synopsis Record for vessels that only engage in domestic voyages. Many of the comments stated that the information

was already on board the vessel and readily available. A few comments were in favor of requiring the information for domestic vessels stating that if the information were in one place it would be useful. While we believe that having the information in one document would be helpful in certain instances, we feel that the value added by requiring another document to be carried on a domestic vessel is not sufficient to do so. The information on the Continuous Synopsis Record is currently maintained on the Certificate of Inspection and the Certificate of Documentation, both of which are required to be on a vessel when it is operating. Therefore, we believe that the requirement should not be extended to domestic vessels and, in the Vessel Security requirements found elsewhere in today's Federal Register, we have only applied the requirement to those vessels obligated to meet the SOLAS requirement.

35. Security Alert System Requirement. In our notice of meeting, we discussed the SOLAS amendments that created a new regulation in Chapter XI-2 (regulation 6) that requires vessels to have a security alert system. The Coast Guard is considering applying the requirement to vessels limited to domestic voyages that are engaged in the transport of certain dangerous cargos. We discussed our intention to extend the application of this requirement to

vessels on international voyages and also requested comment on whether this type of system could be useful on certain domestic voyages such as those involving the transportation of certain dangerous cargos or large passenger vessels.

Many commenters supported extending the requirement to other cargoes and noted the need for alerting us if there were any problems in a quick and efficient manner. In contrast, many other commenters strongly opposed the extension of this system to the domestic fleet and questioned the functionality of it; asking what would be the resulting action once an alert was sent, especially from a remote location. Additionally, some commenters stated a desire to voluntarily install the equipment and use the system once it has been proven effective on a large scale.

While we believe an alert system is a valuable way to communicate to law enforcement if a vessel operator perceives a threat or a security incident is imminent, alternatives can also be used that may also prove effective (such as code words in a routine radio call or a pre-designated call word). Until vessel plans and AMS Plans are established and exercised to evaluate communications and identify gaps, we do not intend to extend this requirement to domestic vessels. However, if future

communication exercises prove that alert systems already within the maritime community do not adequately address the appropriate vessels, we may require them in a separate rulemaking. Therefore, in the Vessel Security requirements found elsewhere in today's Federal Register, we have only applied the requirement to those vessels obligated to meet the SOLAS requirement.

36. Fixed and Floating Platforms Requirements. The International Maritime Organization issued a resolution titled, "Establishment of Appropriate Measures to Enhance the Security of Ships, Port Facilities, MODUs on Location and Fixed and Floating Platforms not covered by Chapter XI-2 of the 1974 SOLAS Convention" which was adopted by the Conference on Maritime Security as Resolution 7 on December 12, 2002. This resolution encourages Contracting Governments to consider security requirements for these maritime operators and platforms. In the notice, we discussed these international efforts and requested comments on whether security requirements should be placed on the offshore fixed and floating platforms.

Many comments were received which emphasized that fixed and floating platforms should be addressed within the port security plan. However, some commenters disagreed stating that even if included in a port security plan, the

degree of security would be very different among platforms due to the potential for different enforcement procedures. Other commenters supported the position that while security measures are appropriate for MODUs and fixed and floating platforms, but believed that any regulations should be carefully tailored to the unique operating environment of the offshore oil and natural gas exploration industry. These commenters also noted that, in their opinion, only a minimal amount of offshore platforms actually pose a viable security risk.

In accordance with the MTSA, we conducted an initial assessment on vessels and U.S. facilities as discussed in the Applicability of National Maritime Security Initiatives section above. Working with the Mineral Management Service (MMS) we identified certain operational quantities and personnel thresholds that are at a higher risk of a transportation security incident. Therefore, in the OCS Facility Security requirements found elsewhere in today's Federal Register, we have only applied requirements to those offshore platforms. However, we are also concerned about the consistency of security measures throughout the offshore community and have worked extensively with industry to develop standards that substantially improve security for this industry. The American Petroleum

Institute (API) recommended practice titled, "API RP70 Security for Offshore Oil and Natural Gas Operations, 1st Edition" is available and its use is strongly encouraged for all owners and operators in this industry. Other platforms not included in the narrow operational category discussed above will be covered as part of the AMS Plan requirements in the "Area Maritime Security" (USCG-2003-14733) interim rule found elsewhere in today's Federal Register. However, in the future, we intend to review the need for further security requirements related to the offshore industry and may require compliance with industry standards such as API RP70 under a separate rulemaking.

37. Seafarers' Identification Criteria Requirements. In our notice of meeting, we noted the MTSA (46 U.S.C. section 70111) requires the Secretary to establish enhanced crewmember identification. In addition, section 103 of the MTSA encourages the Secretary to negotiate an agreement for an international system of identification for seafarers. The Coast Guard has been working with other agencies of DHS (e.g., TSA and Immigration and Naturalization Service), the Department of State, the Maritime Administration, and others to support the work of International Labour Organization (ILO). In the notice, we stated our intent to await the outcome of the June 2003 ILO conference prior to

developing further seafarer identification domestic policy. Because this interim rule has been published in a timeframe that did not allow us to incorporate the results of the ILO conference into it, we will issue any further requirements pertaining to seafarer identification under a separate rulemaking, if appropriate.

In addition to the above, the U.S. Government is mandated through the MTSA (46 U.S.C. 70105) to develop and implement a Transportation Security Card to control access to secure areas on a vessel or facility. Other agencies of DHS (e.g., TSA) have been developing the TWIC to satisfy the MTSA requirement. Pilot testing of the TWIC is scheduled for two ports, each in communication with a Transportation Security Administration central control point. This pilot project allows the other agencies of the DHS (e.g., TSA) to leverage key regional stakeholders and analyze life cycle and cost benefits, as well as the performance of various forms of identification technologies.

Recognizing that the implementation of the TWIC and the ILO efforts on seafarers identification involve substantial negotiation and development, we requested comments on our existing clarification of regulations notice titled "Maritime Identification Credentials"

published in the Federal Register on April 7, 2002(67 FR 51082). This document can be viewed on the DOT Document Management System at http://dms.dot.gov under Docket # USCG-2002-12917. We requested comments in the notice of whether changes to this clarification were needed or if other forms of identification should be recognized in the interim.

Many commenters suggested that we accept merchant mariner documents (MMD) and facility-issued ID cards as a form of identification. Some commenters stated that the existing requirements the Coast Guard set out in its clarification notice are sufficient until the TWIC project is complete. The majority of commenters submitted specific recommendations or suggestions with regard to the TWIC.

Under the current clarification notice, identification such as an MMD or a facility-issued card meeting the requirements set out in the notice are acceptable. Based on the lack of comments requesting amendments to the clarification, we will not amend the requirements at this time. We have incorporated them into this interim rule in order to ensure personal identification is addressed in subchapter H. We will also continue furthering the identification efforts at ILO and through the TWIC project. Comments received on this docket that relate to the TWIC

project have been forwarded to the Transportation Security Administration's docket on that subject for consideration under that rulemaking, as appropriate.

38. Advanced Notice of Arrival (ANOA) Requirements. In our notice of meeting, we discussed that the Coast Guard had a notice of proposed rule titled "Notification of Arrival in U.S. Ports" published in the Federal Register on June 19, 2002 (67 FR 41659). In the meeting notice, we discussed our intent to review the notification requirements based on the additional provisions contained in the SOLAS amendments and the ISPS Code and asked for comments relating to these provisions (specifically SOLAS Chapter XI-2 Regulation 9). Additionally, we requested comments on how foreign flag vessel owners or operators could provide us advance notification on their compliance with the ISPS Code, part B. Finally, we asked if any notification requirements for the upper Mississippi River (above mile marker 235) should be considered for security purposes.

Several commenters suggested that it would be difficult for the vessel to provide the proper information mentioned in the SOLAS amendments or the ISPS Code. Several other commenters stated that the ANOA would be the proper place for a vessel to affirm that it is in

compliance with the ISPS Code. Several comments were submitted with respect to the NOA rulemaking published in the Federal Register on June 19, 2002(67 FR 41659). Several commenters expressed reservation at the value of requiring ANOA above mile marker 235 on the Mississippi river or any other remote locations and suggested it not be required.

We have reviewed the issue and currently believe that an alternative process being developed locally could be more effective. We are incorporating notice of arrival requirements in the Vessel Security interim rule found elsewhere in today's Federal Register to capture the information needed to assess a vessel's compliance with the security requirements of SOLAS Chapter XI-2 and the ISPS Code. The reporting requirements are similar to those required when the International Safety Management Code was implemented and will allow us to have the basic information needed for the evaluation of vessel's security compliance prior to the vessel entering port. Since the publication of the notice of meeting, the Coast Guard published its final rulemaking titled "Notification of Arrival in U.S. Ports" published in the Federal Register on February 28. 2003 (68 FR 9537). Comments submitted to the public meeting notice that related to the proposed Notification of

Arrival (NOA) rulemaking docket were not considered, because the proposed rulemaking comment period for the NOA rulemaking closed prior to the end of the public meeting notice comment period. As for the Mississippi River above mile marker 235 and other remote location reporting requirements, the interim rule does not add any further requirements to the notice of arrival requirements. We will continue reviewing notice of arrival information and the reporting requirements in the future to determine if further requirements are needed to ensure the security provisions are covered. Any additional requirements would be proposed in a future rulemaking.

39. Foreign Port Assessments. In our notice of meeting, we discussed Section 102 of the MTSA (46 U.S.C. section 70108) which requires the Secretary to assess the effectiveness of antiterrorism measures maintained at a foreign port that serves vessels departing on a voyage to the U.S. In the notice, we discussed the concept of accepting a foreign government's approval of the respective port facility security plans, thereby attesting to their compliance with SOLAS and the ISPS Code, to provide the initial assessment of that foreign port's antiterrorism security. We also suggested that we were considering any other relevant information or the possibility of conducting

audits in foreign ports and requested comments on these ideas.

Several commenters stated that accepting the foreign government's approval of a port facility security plan supports the international provisions and places the responsibility in the proper place. Many commenters did ask how the U.S. would keep track of those not meeting their obligations internationally with respect to the port facility requirements in SOLAS Chapter XI-2 and the ISPS Code. Many commenters also stated that the level of compliance of a facility would be directly related to the importance the Contracting Government places upon their obligations to meet the ISPS Code requirements.

It is each Contracting Government's responsibility to ensure compliance; however, it remains our intent to verify the compliance of foreign port facilities in the future and we will work with relevant Contacting Governments to facilitate these evaluations. In the "Area Maritime Security" (USCG-2003-14733) interim final rule found elsewhere in today's Federal Register, recognition of another Contracting Government's port facility security plan is discussed. However, as mentioned, those vessels calling on foreign port facilities that do not meet the requirements of SOLAS and the ISPS Code may be subject to

control and compliance measures, even if the vessel itself has a valid ISSC and an approved security plan.

40. Automatic Identification System (AIS) Requirements. In our notice of meeting, we discussed regulation V/19 of SOLAS, which sets forth the international requirements for the carriage of AIS, including an implementation schedule that was recently accelerated by the newly adopted amendments to SOLAS. Domestically, section 102 of the MTSA (46 U.S.C. section 70114) gives the Secretary additional broad discretion to require AIS on any vessel operating on the navigable waters of the U.S. if necessary for the safety of navigation. In the notice, we discussed our consideration of AIS for security purposes as an essential element in ensuring the safety of navigation. We also noted that the Department of Transportation's Fall 2002 Unified Agenda (67 FR 74853, December 9, 2002), reflected a separate AIS notice of proposed rulemaking (NPRM) which we anticipated publishing during the early months of 2003. However, since the SOLAS amendments made in December 2002 and the MTSA enactment directly impacted this intended notice of proposed rulemaking, which had not taken into account the provisions of the MTSA, we withdrew the NPRM from consideration to assess the impact of both and evaluate options for further

development. We did ask for comments in the notice of public meetings on whether certain vessel types currently listed in the MTSA AIS requirements should be considered candidates for exemption or if the MTSA AIS application was too limited and should be expanded. We also requested comments on whether there are navigable waters of the U.S. where the AIS carriage requirement should be waived because no security benefit would be derived from the requirement.

Several commenters stated that they believed small passenger vessels should not be required to carry AIS due to the equipment expense. Several other commenters asked that certain vessel types such as fleeting tugs, commercial assistance tugs, barges, and vessels of gross tonnage less than 300 on domestic voyages be exempted from the regulations. In contrast, a few commenters suggested that all vessels be required to carry AIS. Several other commenters provided specific areas and types of operations where the system would be beneficial. A series of commenters asked what the policy would be if the SOLAS dates and the MTSA dates were in conflict. Several comments also suggested that vessels operating on remote waterways not be required to carry the system because it was not of any value to the safe navigation of the vessel.

We believe that the MTSA AIS application is consistent with SOLAS and the domestic application is appropriate for the safety and security of navigation within our ports and waterways. Therefore, we have included this application in the AIS interim rule and notice for comment found elsewhere in today's Federal Register. We have also included a process for vessel owners and operators to request to waive or exempt the AIS requirements.

Several comments were submitted that did not reflect the questions asked; however, a few are germane to the general subject of security. A few commenters asked how the Coast Guard intends to receive the AIS signal. A few commenters questioned the security of AIS and stated that they believed it could be used against a vessel or a port by terrorists; these comments went on to suggest that AIS had no benefit from a security aspect and was not applicable. Several commenters also proposed alternatives to AIS at different MARSEC Levels. Finally, a few commenters strongly suggested that we not require AIS in an interim rule but rather issue a notice of proposed rulemaking to ensure adequate notice and comment for this equipment requirement.

We believe that there are quantifiable security and safety benefits from AIS. We are currently upgrading the

Vessel Traffic Service (VTS) systems within the ports to be able to receive and process AIS information. As for the security of AIS, the signal is not secure however; we believe that the benefit of being able to quickly identify and warn mariners about threats directly related to their vessels out weighs the potential security gap presented by AIS's open broadcast nature. We are not considering alternates to AIS for those vessels that are not included in the MTSA requirements but have requested comments on the AIS equipment standards and requirements as well as nationwide implementation in the notice for comments on AIS that is found elsewhere in today's Federal Register. In the future, we may explore other long range tracking alternates and we will continue work in expanding AIS functionality (e.g., long range communication interfacing) and progeny (e.g., AIS Class A derivatives, AIS Class B), in pursuit of other options for those vessels not required to have AIS though could benefit from the safety and security aspects of this technology.

We thoroughly considered the option of issuing a notice of proposed rule for AIS prior to issuing the interim rule found elsewhere in today's Federal Register. Based on the strong language of section 102(d) of the MTSA, which includes "The Secretary shall issue an interim final

rule as a temporary regulation implementing this section ... as soon as practicable after the date of enactment of this section, without the regard to the provisions of chapter 5 of title 5, ...", we determined that AIS, as part 102, needed the same accelerated treatment as the other security requirements presented in the interim rules issued by the Coast Guard and found elsewhere in today's Federal Register. We have provisions for comments to this interim rule and will consider your input prior to the final rulemaking. Additionally, we have included a separate notice of comment found elsewhere in today's Federal Register to ensure that vessel owners and operators are afforded ample opportunity to comment on this equipment carriage requirement in the broad nationwide application that MTSA suggests.

Discussion of Interim rule

This Interim rule establishes parts 101 and 102 in new subchapter H to title 33 of the Code of Federal Regulations. It provides the General Provisions for all of subchapter H, and is broken down into five subparts, which we will now discuss in order.

Part 101 - Subpart A – General.

Subpart A, section 101.100 explains the purpose behind all of the Regulations found in subchapter H. That purpose

is to increase the level of maritime security found in our nation's ports, while at the same time aligning our domestic maritime security regulations with international standards, wherever such alignment is appropriate. These regulations should dissuade those persons or groups that would seek to disrupt the maritime elements of the national transportation system by ensuring that security arrangements are as compatible as possible for vessels trading internationally.

Subpart A, section 101.105 goes on to define the terms that are used in subchapter H. Definitions found in this section of part 101, subpart A are applicable to the entire subchapter. We have included all definitions in part 101 in order to give the reader a common place for reference, a "one stop shopping" of sorts.

Many of the definitions are self-explanatory, so we have not gone into detail about them here. For brevity, we are limiting this discussion to those definitions that we think may be confusing or novel. For instance, the MTSA and the ISPS Code use different terms to define similar, if not identical, persons or things. These differing terms sometimes match up with the terms used in subchapter H, but sometimes they do not. Thus, in some definitions you will find references to other terms, used in the MTSA or the

ISPS Code. We are including a table of these terms here, for easy reference.

Table 4 Equivalent Terms.

Subchapter H Terms	USCG Terms	MTSA Terms	ISPS Code Terms
PLANS			
Area Maritime Security (AMS) Plan	Port Security Plan	Area Maritime Security Transportation Plan	Port Facility Security Plan
Vessel Security Plan	Vessel Security Plan	Vessel Security Plan	Ship Security Plan
Facility Security Plan	Facility Security Plan	Facility Security Plan	(None)
ASSESSMENTS			
Area Maritime Security (AMS) Assessment	Port Security Assessment	(None)	Port Facility Security Assessment
Vessel Security Assessment	Vessel Security Assessment	Vessel Security Assessment	Ship Security Assessment
Facility Security Assessment	Facility Security Assessment	Facility Security Assessment	None
PEOPLE			
Captain of the Port (COTP)	Captain of the Port (COTP)	Federal Maritime Security Coordinator (FMSC)	Port Facility Security Officer (PFSO)
Company Security Officer	Company Security Officer	Company Security Officer	Company Security Officer
Vessel Security Officer	Vessel Security Officer	Qualified Individual	Ship Security Officer
Facility Security Officer	Facility Security Officer	Qualified Individual	None
Area Maritime Security (AMS) Committee	Port Security Committee	Area Maritime Security Advisory Committee	None

We defined "company" broadly in order to ensure that we captured all persons and/or legal entities that may in fact own or operate a vessel or facility under this subchapter. We did not list out specific legal entities, in order to avoid unintentionally omitting one, making enforcement more difficult as new legal entities are

created. We interpret our definition to include the following legal entities: corporations, partnerships, business trusts, associations, joint ventures, sole proprietorships, and unincorporated organizations.

We chose the term "dangerous substances and devices" for specific reasons. The ISPS Code uses the phrase "weapons, dangerous substances or devices" when identifying the intent of certain security measures. We use dangerous substances and devices because these interim rules do not prohibit weapons that are carried in accordance with the applicable local, State, or federal laws. However, vessel or facility owners or operators, in their own proprietary capacity, may prohibit lawfully possessed weapons as a condition of carriage/entrance. They may also develop and implement procedures whereby weapons and ammunition are temporarily relinquished to the vessel or facility owner or operator and placed in a secure location for the duration of the voyage or stay at the facility. The Coast Guard will retain the authority to impose restrictions on owners or operators when necessary to ensure safety or security, or to secure the observance of rights or obligations of the U.S., especially at heightened threat conditions. The Coast Guard is working with DHS (e.g., TSA) to develop an intermodal policy regarding items that passengers may be

prohibited from carrying. The policy is still being developed but may affect the carriage of certain weapons onboard certain passenger vessels.

We defined "international voyage" to include those vessels that solely navigate the Great Lakes and the St. Lawrence River as far east as a straight line drawn from Cap des Rosiers to West Point, Antiocosti Island and, on the north side of Anticosti Island, the 63rd meridian.

We chose to apply length thresholds using the definition of "registered length" instead of overall length, under the authority of 46 U.S.C. 70114 (2). This was done to facilitate enforcement and minimize confusion for vessel owners. Registered lengths are assigned for all documented vessels of the U.S. and appear in Coast Guard databases and on Certificates of Documentation. Conversely, overall lengths can vary as a function of voyage type, and are not assigned for all documented vessels of the U.S. In many cases the two definitions coincide, and where they do not coincide, the registered length is slightly less than overall length.

We have expressed gross tonnage thresholds in one of two ways. If the threshold must be applied using the vessel's gross tonnage measurement under 46 U.S.C. Chapter 143, Convention Measurement, the threshold is expressed in

terms of "gross tonnage, ITC." If the threshold must be applied using the vessel's gross tonnage measurement under 46 U.S.C. Chapter 145, Regulatory Measurement, the threshold is expressed in terms of "gross register tons." For those vessels that only a have gross tonnage, ITC measurement, yet the requirement calls for a gross register tons threshold, then the gross tonnage, ITC measurement must be used.

We have included a definition of the phrase "Maritime Security (MARSEC) Level," as well as definitions for each individual MARSEC Level. MARSEC Level, in general, refers to the prevailing threat environment to the maritime elements of the national transportation system. As the threat of a transportation security incident increases, the individual MARSEC Level moves higher, from one to three. Additional discussion on the concept of MARSEC Levels and how they interplay with DHS's HSAS is included below in the discussion for subpart B.

We have also defined a new document, called a Maritime Security (MARSEC) Directive. All MARSEC Directives will qualify as SSI under 49 CFR 1520.7 of the Transportation Security Administration interim rule on SSI, that will be published in the near future. Once published, we will post a copy of this interim rule to the docket. The Coast Guard

MARSEC Directives will be consistent with the National Transportation System Security Plan (NTSSP) and in accordance with Transportation Security Directives, as established by the Transportation Security Administration. Additional discussion on what a MARSEC Directive is, how MARSEC Directives will be issued and the proper response to a MARSEC Directive is included below in the discussion for subpart D.

We have adopted the MTSA definition for "transportation security incident." We also adopted the ISPS Code definitions for "Company Security Officer" and "Vessel Security Officer." Using these two definitions as our basis, we were able to also define "Facility Security Officer."

We have also defined the phrase "waters subject to the jurisdiction of the U.S." to include the navigable waters of the U.S., the Exclusive Economic Zone (EEZ), the seabed and subsoil of the OCS of the U.S. and the resources thereof and the waters adjacent thereto.

Subpart A section 101.110 sets the applicability for all of subchapter H. As stated, it is very broad, covering all vessels, structures, and facilities of any kind, located in, on, or adjacent to waters subject to the jurisdiction of the U.S. This broad application is

necessary to cover all entities affected by at least one part of new subchapter H. Each individual part contains a separate applicability section, which is more narrow than that contained in the General Provisions of part 101.

In section 101.115 we have incorporated by reference the ISPS Code, 2003 Edition. Specifically, we are incorporating the amendments adopted on 12 December 2002 to the Annex to The International Convention for SOLAS, 1974 and the ISPS Code, parts A and B, also adopted on 12 December 2002. The material is incorporated for all of subchapter H.

Sections 101.120 and 101.125 of subpart A reflect the flexibility that the Coast Guard has tried to build into these regulations. Section 101.120(a) reflects one of the SOLAS amendments, and allows the U.S. to agree upon alternative security arrangements with other SOLAS contracting governments, but only to cover short, international voyages on fixed routes between facilities subject to the jurisdiction of the U.S. and facilities subject to the jurisdiction of the other contracting government. Any vessel covered by one of the agreements is prohibited from engaging in any vessel-to-vessel activity, unless it would be conducting the vessel-to-vessel activity with another vessel covered by the same agreement.

Section 101.120(b)-(c) allows applications for approval of Alternative Security Programs. As noted in the discussion of comments section above, we received many comments supporting the idea of allowing vessels or facilities to submit security plans or programs that meet, as an example, an industry standard, instead of requiring them to follow the plan requirements included in this subchapter, SOLAS, or ISPS Code, parts A and B. We have, accordingly, built this flexibility into the regulation. Once an Alternative Security Program is approved, it will be added to Section 101.125. An up-to-date list will also be kept by G-MP, and will be accessible on the Internet.

Section 101.120(c) details the information that must be included in an application for approval. Part of that application includes an assessment of what vessels or facilities may use the proposed Alternative Security Program. This is important because not all Alternative Security Program will be appropriate for all vessels or facilities. For example, not all approved Alternative Security Programs for facilities will fit the security planning requirements necessary for a CDC facility. As part of the approval process, the Commandant will indicate, in his approval letter, those types of vessels or

facilities that may use the approved Alternative Security Programs.

Section 101.130 allows the Commandant to accept equivalent security measures, so long as they are at least as effective as those that are mandated in subchapter H, SOLAS, or ISPS Code, parts A and B. This allowance is made for both vessels and facilities required to have security programs under parts 104, 105, or 106. Equivalent security measures differ from Alternative Security Programs. Once an Alternative Security Program is approved, any vessel or facility that meets the approval qualifications may meet the provisions of the Alternative Security Program in lieu of meeting the security plan requirements of the applicable part of this subchapter. Equivalent security measures, once approved, are only approved for the particular vessel or facility making the application.

Equivalent security measures are those distinct security measures, such as fences or alarm systems, which may be required within a security plan. Requests for approval of equivalent security measures should be made at the time that a vessel or facility is submitting their security plan for approval, and they should be made to the appropriate plan approval authority under part 104, 105, or 106.

Part 101 - Subpart B – Maritime Security Levels.

The SOLAS Amendments and ISPS Code lay out a series of requirements for Contracting Governments and Administrations to mandate security levels that are appropriate for their vessels and ports. The Coast Guard is implementing these requirements in coordination with the HSAS. Homeland Security Presidential Directive (HSPD)-3 defines a five-tiered system for setting threat levels. We are implementing MARSEC Levels, which directly correspond to the security levels as discussed in the SOLAS amendments and the ISPS Code. The MARSEC Levels will be linked to the HSAS as shown in the table below. This table is also included in the regulation itself.

Table 5: Relation Between HSAS, MARSEC Levels and SOLAS-required Security Levels.

Homeland Security Advisory System (HSAS) Threat Condition		Equivalent Maritime Security (MARSEC) Level	Equivalent SOLAS-required Security Level
Low Elevated Guarded	Green Blue Yellow	Maritime Security Level 1	Security Level 1
High	Orange	Maritime Security Level 2	Security Level 2
Severe	Red	Maritime Security Level 3	Security Level 3

At all times, the Commandant retains the discretion to adjust the MARSEC Level when necessary to address any particular concerns or circumstances related to the maritime elements of the national transportation system. Additionally, the COTP retains the authority to temporarily raise the MARSEC Level for his/her AOR, or a specific segment thereof, when necessary to address exigent circumstances immediately affecting the security of the maritime elements of the national transportation system within his/her AOR.

Part 101 - Subpart C – Communication.

Subpart C, section 101.300 details the methods the COTP will use to communicate changes in the MARSEC Level. Note that individual ATMS Plans may outline additional communication methods that are particular to the Plan's covered area. It also details the threat information that the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities located within his or her AOR. Finally, this section requires vessel and facility security plan holders to confirm that they have implemented the measures and/or actions in their security plans that correspond to the MARSEC Level.

Subpart C, section 101.305 describes the reporting requirements placed on vessel and facility security plan

holders. First, it requires that they report suspicious activities that may result in a transportation security incident. These reports are to be made to the National Response Center (NRC), and the regulation lists several methods of contacting the NRC. We also require that security plan holders call the NRC to report breaches of security. This captures a broader range of activities that, while not severe enough to pose a threat of a transportation security incident, are still considered serious. Examples of breaches of security include attempts to smuggle dangerous substances or devices onto a facility or vessel, attempts to break into the facility or vessel, or attempts to tamper with, alter, or mix cargos. They would not, however, include acts of vandalism.

It is advised, although not required, that vessel and facility security plan holders familiarize themselves with the type of information that will be asked of them when placing a call to the NRC. They may do this by visiting the NRC's website at www.nrc.uscg.mil, clicking on "Services," then clicking on "Online Reporting." This will call up a menu of several different types of incidents, such as vessel, pipeline, and aircraft. Clicking on any of these types will open the reporting form.

This section also encourages other persons or entities to call the NRC to report suspicious activities that may result in a security incident.

Vessel and facility security plan holders are also required to report the onset of an actual transportation security incident to their local COTP or, if a facility regulated by part 106 of this subchapter, their District Commander. They must also immediately begin implementing the provisions of their security plan, including contacting any other individuals or entities (such as the NRC or local authorities) listed within their security plan.

Section 101.310 of subpart C lists two methods of communication, alert systems and AIS, which may be used to augment the communications methods listed in a vessel's security plan. Alert systems are discussed in more detail in part 104 of this subchapter; AIS is covered in 33 CFR parts 26, 161, 164 and 165.

Part 101 - Subpart D – Control Measures for Security.

This section also explicitly states that the provisions of subchapter H do not limit the powers conferred by any other law or regulation upon any Coast Guard commissioned, warrant, or petty officer.

Subpart D, section 101.405 describes when the Coast Guard will issue a Maritime Security (MARSEC) Directive.

MARSEC Directives will set mandatory measures that all defined entities must meet in a specified time. These entities will also be required to verbally confirm, to the local COTP or District Commander (as appropriate), receipt of the MARSEC Directive, as well as specify the method by which the mandatory measures have been (or will be) met. This section also builds in some flexibility by allowing the MARSEC Directive recipient to submit proposed equivalent security measures to the local COTP or District Commander (as appropriate), if the MARSEC Directive recipient is unable to implement the measures mandated in the MARSEC Directive. However, the entity will only be able to propose such alternatives for the length of time specified in the MARSEC Directive, and he/she will be required to implement any alternative measure that the COTP does approve.

The Coast Guard plans to use MARSEC Directives to mandate additional security measures that are SSI. They may be applicable to all maritime elements of the national transportation system, or they may impose additional security measures on specific maritime elements of the national transportation system. As stated, only the Commandant or his/her delegate will issue these MARSEC Directives at the national level. All MARSEC Directives

will be designated and disseminated as SSI, in accordance with 49 CFR part 1520 (to be amended by the Transportation Security Administration). As a result, the MARSEC Directives will only be issued to those persons who can demonstrate that they are a covered person and that they have a need to know, as those terms are defined in the SSI regulation. Company, Vessel, and Facility Security Officers should familiarize themselves with the SSI regulation.

When a new MARSEC Directive is issued, the Coast Guard plans to publish, in the Federal Register and through other means (local notices to mariners, press releases, etc.), that it has issued a new MARSEC Directive. The MARSEC Directives will be individually numbered, and will be assigned to a series that corresponds with the part of this subchapter to which the MARSEC Directive refers. For example, the first MARSEC Directive addressing a new requirement for vessels regulated under part 104 of this subchapter would be identified as MARSEC Directive 104-01.

Upon receiving notice that a new MARSEC Directive has been issued, affected entities would contact or be contacted by their local COTP (or, if appropriate, their District Commander) to receive a copy of the MARSEC Directive. The COTP or District Commander will confirm,

prior to distributing the MARSEC Directive, that the requesting entity is a covered person with a need to know, and that the requesting entity will safeguard the MARSEC Directive as SSI. Thus, continuing with the example from the previous paragraph, upon receiving notice that an MARSEC Directive in the 104 series has been issued, owners and operators of vessels covered by part 104 of this subchapter would need to contact their local COTP to obtain a copy of the MARSEC Directive. They would then be required to comply with the MARSEC Directive, or follow the procedures set out in the MARSEC Directive for gaining approval of an equivalent security measure. COTPs may also use the AMS Committee as a mechanism for disseminating the MARSEC Directive to those with a need to know.

MARSEC Directives will be issued under an extension of the Coast Guard's existing COTP authorities regarding maritime security, found in 33 U.S.C. 1226 and 50 U.S.C. 191. In part, the implementing regulations for 50 U.S.C. 191, found at 33 CFR 6.14-1 and promulgated by Executive Order 10277, contemplate action by the Commandant that is national in scope. Specifically, these regulations authorize the Commandant to prescribe such conditions and restrictions deemed necessary under existing circumstances for the safety of waterfront facilities and vessels.

Additionally, 43 U.S.C. 1333(d) authorizes the Coast Guard to establish certain requirements for OCS facilities. Moreover, MARSEC Directives are a necessary and integral part of exercising the Coast Guard's authorities in 46 U.S.C. Chapter 701, to ensure that that Chapter's security requirements are met.

The MARSEC Directives will provide specific instruction to the regulated maritime community to achieve the performance standards required by this subchapter and 46 U.S.C. Chapter 701. For example, the plans required by 46 U.S.C. 70103 are not subject to public disclosure, in accordance with 46 U.S.C. 70103(d), and contain SSI that, if disclosed, could be used to subvert or exploit the security program for vessels, facilities, OCS facilities, or ports. This could include passenger screening levels, means of monitoring restricted areas, and other requirements that may be necessary to ensure that the security plans remain viable. Like civil aviation security, these specific requirements cannot be placed in a public regulation and are better suited for issuance through a MARSEC Directive that is itself not subject to public disclosure.

Since MARSEC Directives would be issued when necessary to protect national security and to preserve the rights and

obligations of the U.S. with regarding maritime security, the Coast Guard has determined that the issuance of MARSEC Directives do not fall within the requirements of the Administrative Procedure Act by virtue of the military and foreign affairs exemption (5 USC 553(a)(1)). Furthermore, the basis for the MARSEC Directive would also constitute "good cause" within the meaning of the Administrative Procedure Act (5 USC 553(b)(3)(B) and (d)(3)) regarding notice and comment rulemaking and effective dates since it would be contrary to the public interest and impracticable to provide SSI relating to maritime security and methods of detection, deterrence, and response in a public forum.

Subpart D, section 101.410 lists examples of the types of control and compliance measures that a COTP may take on vessels and/or facilities within his/her AOR that are not in compliance with subchapter H. The lists of measures are not meant to be exhaustive. This section also notes that the COTP may impose one or more of these control and compliance measures on a vessel that is in compliance with subchapter H, if that vessel has called on a facility that is not in compliance, or if it has called on a port that does not maintain adequate security measures to ensure that the level of security achieved by subchapter H has not been compromised.

Section 101.415 outlines the penalty provisions that may be taken against persons for violating the provisions of this subchapter. Civil and criminal penalties may be imposed under 33 U.S.C. 1232 or 50 U.S.C. 192, as appropriate, for violations of control and compliance measures, including COTP orders and security zones. This simply restates the current law applicable under the Magnuson Act, 590 U.S.C. 191, implemented at 33 CFR part 6, and the Ports and Waterways Safety Act, 33 U.S.C. 1221 et seq., implemented in part at 33 CFR parts 160 and 165. Pursuant to 46 U.S.C. 70117, civil penalties may also be assessed for non-compliance with any other requirement in this subchapter, including those imposed by a MARSEC Directive.

Finally, section 101.420 outlines the appeal rights available to persons directly affected by a decision or action taken by the COTP or the Commanding Officer of the Marine Safety Center.

Part 101 - Subpart E – Other Provisions.

Subpart E sets out the remaining regulations that apply to all of subchapter H that do not fit in any of the subparts discussed above. We have reserved the first section in this subpart for procedures for authorizing a Recognized Security Organization (RSO). As noted above in

the discussion of comments, the Coast Guard is authorized, under SOLAS, to delegate its assessment and plan approval authority to an RSO. The Coast Guard has decided to retain this authority for the time being. We may, however, delegate some (or all) of this authority to RSOs in the future. As a result, we are reserving this section for outlining the procedures an organization will need to follow in order to qualify as an RSO in the future.

Section 101.505 describes the purpose behind a Declaration of Security (DoS). A DoS is intended to clarify the specific security responsibilities of a vessel and a facility (or another vessel) with which it will be conducting some activity. It will be used to eliminate situations where confusion leads the vessel to believe that the facility (or other vessel) will take care of certain security measures, while the facility (or other vessel) believes that the vessel will take care of the same security measure. Parts 104 through 106 of subchapter H describe in detail the who, what, where, when and how of completing a DoS for their respective regulated entities. Additionally, to ensure that vessels and facilities coordinate security during special marine events such as festivals that draw large numbers of people to the waterfront or vessels that wish to enter port with a higher

MARSEC Level than what has been set for the port, we have included a provision to ensure the COTP's ability to mandate a DoS.

Section 101.510 of subpart E lists the various assessment tools that may be used to meet the risk assessment requirements in parts 103 through 106 of this subchapter. This list is provided to ensure that security assessments done to meet these requirements are consistent with other modal assessments and are sufficient enough to enable the development of security plans. We have been working with other agencies to develop assessment tools that are sensitive to a diversity of transportation modes to ensure equity of security throughout the entire National transportation system. We anticipate that eventually one security assessment tool will be mandated for all transportation modes. In the interim, the list provided in Section 101.510 enables the maritime security provisions to advance until the national transportation security assessment mandate is complete. Even when a national transportation security assessment is in place, we intend to provide a "grandfather clause" to those security assessments done to meet the maritime security requirements found elsewhere in today's Federal Register.

The Transportation Security Administration intends to publish a Notice of Proposed rulemaking with request for comment that promulgates rules in 49 CFR part 1574 to manage the access to and use of a user-friendly risk-based vulnerability assessment tool. This tool will be the result of inter-agency work, under the leadership of TSA thus far to establish a national transportation security assessment. It will be designed as a self-assessment tool for the owner or operator, and is one of the tools an owner or operator may use to meet the risk assessment requirements in parts 103, 104, 105 and 106 of subchapter H.

Section 101.515 of subpart E prescribes the minimum requirements for personal identification credentials for purposes of access control under this subchapter. As discussed in the Discussion of Comments to Maritime Security Public Meetings section above, these requirements are consistent with the Coast Guard's previous policy notice on maritime credentials acceptable under 33 CFR part 125.

Part 102 – National Maritime Transportation Security Plan.

Part 102 in subchapter H has been reserved for the National Maritime Transportation Security (NMTS) Plan that

is required under 46 U.S.C. 70103a. At this time we are coordinating the implementation of the National Maritime Security Advisory Committee (NMSAC) as required in the MTSA (46 U.S.C. 70112a). While the development of this overarching plan and the establishment of the National Advisory Committee are key sustaining National Maritime Security initiatives, we do not feel their development is necessary prior to the implementation of these interim rule requirements. We believe the concepts found in the interim rules published in today's Federal Register represent the foundation of National Maritime Transportation Security and intend to incorporate them in the development of the NMTS plan. We will promulgate the NMTS plan and Advisory Committee charter and membership requirements under a separate notice and rulemaking in the future.

Additionally, the Aviation and Transportation Security Act (ATSA) assigns responsibility for managing the security of the nation's transportation modes to the Transportation Security Administration. In its role as the National Transportation System Security Manager, Transportation Security Administration intends to develop a National Transportation System Security Plan (NTSSP) to define national strategy and provide tools to help manage risk across the nation's multi-modal transportation system.

The NTSSP will provide a comprehensive and systematic approach to the national transportation system's risk management. It will set the framework and establish goals for National Security Plans for each of the transportation modes.

Incorporation by Reference

The Director of the Federal Register has approved the material in § 101.115 for incorporation by reference under 5 U.S.C. 552 and 1 CFR part 51. You may inspect this material at U.S. Coast Guard Headquarters where indicated under ADDRESSES. Copies of the material are available from the sources listed in § 101.115.

This interim rule incorporates by reference the International Ship and Port Facility Security (ISPS) Code, 2003 Edition. Specifically, we are incorporating the amendments adopted on 12 December 2002 to the Annex to The International Convention for the Safety of Life at Sea (SOLAS), 1974 and The International Code For the Security of Ships and of Port Facilities, also adopted on 12 December 2002. The material is incorporated for all of subchapter H. The interim rule titled "Automatic Identification System; Vessel Carriage Requirement" (USCG-2003-14757), found elsewhere in today's Federal Register, also incorporates material by reference.

Regulatory Assessment

This interim rule is a "significant regulatory action" under section 3(f) of Executive Order 12866, Regulatory Planning and Review, and has been reviewed by the Office of Management and Budget (OMB) under that Order. It requires an assessment of potential costs and benefits under section 6(a)(3) of that Order. It is significant under the regulatory policies and procedures of DHS. A draft assessment is available in the docket as indicated under ADDRESSES.

Summary of Changes in the Cost Assessment from the Meeting Notice

In a December 30, 2002, meeting notice [67 FR 79742], the Coast Guard presented a preliminary cost assessment estimating the cost to the regulated public of implementing MTSA, the ISPS code, and complying with applicable security NVICs. We asked for comments on our estimates and have changed portions of our cost assessments for the interim rules based on those comments.

We received a wide range of comments on the preliminary assessment. In some areas, commenters believed we were overestimating costs, in other areas they believed we were understating costs, and in many instances commenters believed we had accurately accounted for costs.

As a result of the comments, our cost estimates for vessels and facilities increased, while our estimates for ports remained about the same. Additionally, the summary of costs we present below includes estimates for the OCS interim rule and the AIS interim rule, which were not part of our original assessment for the meeting notice.

For vessels, we decreased the population of U.S. flag SOLAS fishing vessels from 39 to 1. We also removed domestic MODUs and domestic freight barges regulated under 46 CFR subchapter I from our assessment, as the Coast Guard is not regulating these vessels in these interim rules. We added 70 foreign vessels that make port calls in the United States but are not subject to SOLAS. We increased the cost for hand-held radios and portable vapor detectors based on information received in the comments.

In our preliminary assessment, we assumed that equipment would be replaced every 10 years. Several commenters believed that this underestimated the replacement costs for several of the pieces of equipment that we considered. Specifically, several commenters stated some equipment would be broken, lost, or stolen before the 10-year replacement. We agreed that we should increase equipment costs to account for these situations. Because the replacement cycle of equipment will vary

considerably among types of equipment and its uses, we increased the annual operations and maintenance (O&M) costs to more accurately capture increased replacement and repair. In the preliminary cost estimates, we assumed that annual O&M costs would be 5 percent of the initial capital purchase cost. In the Cost Assessment for this rulemaking, we increased annual O&M to 10 percent of the initial purchase cost. We also changed the annual cost for Vessel Security Officers to more accurately reflect the annual costs of the mariners that will perform security duties aboard their vessels. The net effect of these changes was to increase initial and annual costs for vessels.

Based on comments, we found there was some confusion about labor costs. Labor costs presented in our assessment are not the hourly wage paid to the employee; rather, they are the fully loaded cost to the company of carrying the position and providing employee benefits. Additionally, there was some confusion about our estimates for Vessel Security Assessments and Vessel Security Plans. We believe that most companies will choose to develop one overarching assessment or plan, and then take that overarching document and add documentation specific to each vessel in their fleets. The "incremental" costs that we presented for each vessel type in the preliminary assessment represented the

cost to add the vessel to the overarching company assessment or plan. Thus, in our preliminary cost assessment it may have seemed that it cost only a few dollars to develop a Vessel Security Assessment or Vessel Security Plan for a particular vessel. In fact, we believe that Vessel Security Assessments and Vessel Security Plans will represent a substantial initial cost, but adding vessels to an overarching plan will be a smaller, incremental cost. For annual updates to Vessel Security Assessments and Vessel Security Plans, we have increased the time required to amend these documents from 1 minute per vessel (0.02 hours) to 15 minutes per vessel (0.25 hours). The net effect of this change was to increase our annual costs slightly.

For facilities, we added certain fleeting areas to our population based on our assessment of the risk these areas pose. We also increased equipment costs for most items for Group A facilities in response to several comments. (We recognize that not all facilities will incur the same cost for personnel salaries, hire the same number of security guards, or spend the same amount of time drafting Facility Security Assessments and Facility Security Plans. For the purpose of this assessment, we have divided the facility population in two groups. One group is composed of one

third of all facilities and will have more security duties, hire more guards, and spend more time drafting Facility Security Assessments and Facility Security Plans than the other group that is composed of the remaining two-thirds of the total population. Facilities in the first group are addressed in this assessment as "A" and facilities in the second group as "B.") As in our vessel assessment, we increased annual O&M costs from 5 percent of purchase cost to 10 percent of purchase cost to more accurately capture annual repair and replacement. We received several comments on the cost estimated for security guards. Commenters stated the $40,000 annual cost presented was either too low, too high, or accurate. We believe these diverging opinions could be explained by the cost of living and the corresponding wage variation among difference regions of the country. The costs presented in the assessment are national averages, and we full expect different regions of the country to pay different wage rates. However, we do believe that the $40,000 per year estimated per security guard may be lower than what could be expected. Consequently, we have revised our estimate from $40,000 per year to $50,000 per year per security guard. Finally, we included the cost of making Declaration

of Security (DoS) annual. The net effect of these changes was to increase initial and annual costs for facilities.

A detailed summary of the changes made from the December 2002 meeting notice and the Cost Assessment for the interim rules for security is presented in Table 6.

Table 6. Summary of Changes Made to Cost Assessment.

Item	December 2002 Meeting Notice	Cost Assessment for IR	Comment
Population of fishing vessels	39 vessels	1 vessel	Revised based on new information from commenter
Population of domestic MODUs	159 vessels	0 vessels	IR will not be applicable to domestic MODUs
Population of domestic freight barges	262 vessels	0 vessels	IR will not be applicable to domestic freight barges regulated under Subchapter I
Population of foreign non-SOLAS vessels	0 vessels	70 vessels	IR will be applicable to these vessels regulated under Subchapter I
Hand-held radio (vessels)	$200 per item	$500 per item	Revised based on comment
Portable vapor detector (vessels)	$8,000 per item	$15,000 per item	Revised based on comment
O&M costs for equipment (vessels)	5% of purchase cost	10% of purchase cost	Revised based on comment
Annual incremental costs to amend VSAs and VSPs	$0.02 per vessel per year	$25 per vessel per year	Revised based on comment
Vessel Security Officers	$5,000 per vessel per year, non-towing vessels only	$8,500 per non-towing vessel per year; $4,250 per towing vessel per year	Revised based on comment
Fleeting areas	0 areas	600 areas	Population added to IR
Communications system (group A facilities)	$300,000 per facility	$400,000 per facility	Revised based on comment
Gates (group A facilities)	$100,000 per facility	$200,000 per facility	Revised based on comment
CCTVs (group A	$130,000 per	$260,000 per	Revised based on

facilities)	facility	facility	comment
Lights (group A facilities)	$200,000 per facility	$400,000 per facility	Revised based on comment
Fencing (group A facilities)	$500,000 per facility	$750,000 per facility	Revised based on comment
Hand-held radio (group A and B facilities)	$200 per item	$500 per item	Revised based on comment
O&M costs for equipment (facilities)	5% of purchase cost	10% of purchase cost	Revised based on comment
Security guard	$40,000 per year	$50,000 per year	Revised based on comment
Declaration of Security	No cost estimated	Cost estimated	Added requirement to IR

Cost Assessment Summary

The following summary presents the estimated costs of complying with the interim rules on Vessel Security, Facility Security, OCS Facility Security, Area Maritime Security, and AIS, which are published elsewhere in today's Federal Register.

For the purposes of good business practice, or to comply with regulations promulgated by other Federal and State agencies, many companies already have spent a substantial amount of money and resources to upgrade and improve security. The costs shown in this summary do not include the security measures these companies have already taken to enhance security.

We realize that every company engaged in maritime commerce would not implement the interim rules exactly as presented in this assessment. Depending on each company's

choices, some companies could spend much less than what is estimated herein, while others could spend significantly more. In general, we assume that each company would implement the interim rules based on the type of vessels or facilities it owns or operates, whether it engages in international or domestic trade, and the ports where it operates.

This assessment presents the estimated cost if vessels, facilities, OCS facilities, and ports are operating at MARSEC Level 1, the current level of operations since the events of September 11, 2001. We also estimate the costs for operating for a brief period at MARSEC Level 2, an elevated level of security. We also discuss the potential effects of operating at MARSEC Level 3, the highest level of maritime security.

We do not anticipate that implementing the interim rules will require additional manning aboard vessels or OCS facilities; existing personnel can assume the duties envisioned. For facilities, we anticipate additional personnel in the form of security guards that can be hired through contracting with a private firm specializing in security.

Based on our assessment, the first-year cost of implementing the interim rules is approximately $1.507

billion. Following initial implementation, the annual cost is approximately $884 million, with costs of present value (PV) $7.348 billion over the next 10 years (2003–2012, 7 percent discount rate). Estimated costs are as follows.

Vessel Security.

Implementing the interim rule will affect about 10,300 U.S. flag SOLAS, domestic (non-SOLAS), and foreign non-SOLAS vessels. The first-year cost of purchasing and installing equipment, hiring security officers, and preparing paperwork is approximately $218 million. Following initial implementation, the annual cost is approximately $176 million. Over the next 10 years, the cost would be PV $1.368 billion.

Facility Security.

Implementing the interim rule will affect about 5,000 facilities. The first-year cost of purchasing and installing equipment, hiring security officers, and preparing paperwork is an estimated $1.125 billion. Following initial implementation, the annual cost is approximately $656 million. Over the next 10 years, the cost would be PV $5.399 billion.

OCS Facility Security.

Implementing the interim rule will affect about 40 OCS facilities under U.S. jurisdiction. The first-year cost of

purchasing equipment and preparing paperwork is an estimated $3 million. Following initial implementation, the annual cost is approximately $5 million. Over the next 10 years, the cost would be PV $37 million.

Port Security.

Implementing the interim rule will affect about 47 maritime areas containing 361 ports. The initial cost of the startup period (June 2003–December 2003) is estimated to be $120 million. Following the startup period, the first year of implementation (2004) is estimated to be $106 million. After the first year of implementation, the annual cost is approximately $46 million. Over the next 10 years, the cost would be PV $477 million.

Automatic Identification System (AIS).

Implementing the interim rule will affect about 4,600 U.S. flag SOLAS and domestic (non-SOLAS) vessels in VTS areas. The first-year cost of purchasing equipment and training for U.S. vessels (SOLAS and domestic) is approximately $40 million. Following initial implementation, the annual cost for U.S. vessels is approximately $1 million. Over the next 10 years, the cost for these vessels would be PV $66 million (with replacement of the units occurring 8 years after installation).

An additional 70 foreign flag, non-SOLAS vessels will also be affected. The first-year cost of purchasing and installing equipment and training personnel for these vessels is approximately $0.6 million. Following initial implementation, the annual cost is less than $0.1 million. Over the next 10 years, the cost for these vessels would be PV $1 million.

Maritime Security Levels 2 and 3.

MARSEC Level 2 is a heightened threat of a security incident, and intelligence indicates that terrorists are likely to be active within a specific target or class of targets. MARSEC Level 3 is a probable or imminent threat of a security incident. MARSEC Levels 2 and 3 costs are not included in the above summaries because of the uncertainty that arises from the unknown frequency of elevation of the MARSEC Level and the unknown duration of the elevation.

The costs to implement MARSEC Levels 2 and 3 security measures in response to these increased threats do not include the costs of security measures and resources needed to meet MARSEC Level 1 (summarized above) and will vary depending on the type of security measures required to counter the specific nature of higher levels of threat. Such measures could include additional personnel or

assigning additional responsibilities to current personnel for a limited period of time.

We did not consider capital improvements, such as building a fence, to be true MARSEC Levels 2 or 3 costs. The nature of the response to MARSEC Levels 2 and 3 is intended to be a quick surge of resources to counter an increased threat level. Capital improvements generally take time to plan and implement and could not be in place rapidly. Capital improvement costs are estimated under MARSEC Level 1 costs.

We did not calculate MARSEC Level 2 cost for the AMS because this will be primarily a cost to the Coast Guard for administering the heightened MARSEC Level in port and maritime areas.

In order to estimate a cost for MARSEC Level 2, we made assumptions about the length of time the nation's ports can be expected to operate at the heightened security level. For the purpose of this assessment only, we estimate costs to the nation's ports elevating to MARSEC Level 2 twice a year, for 3 weeks each time, for a total period of 6 weeks at MARSEC Level 2. Again, this estimate of 6 weeks annually at MARSEC Level 2 is for the purposes of illustrating the order of magnitude of cost we can expect. Our estimate should not be interpreted as the

Coast Guard's official position on how often the nation's ports will operate at MARSEC Level 2.

We estimate that there are Vessel Security Officers aboard all U.S. flag SOLAS vessels and most domestic vessels. We estimate that there will also be key crewmembers that can assist with security duties during MARSEC Level 2 aboard these vessels. We assume that both Vessel Security Officers and key crewmembers will work 12 hours a day (8 hours of regular time, 4 hours of overtime) during the 42 days that the ports are at MARSEC Level 2. We then estimate daily and overtime rates for Vessel Security Officers and key crewmembers. Given these assumptions, we estimate that elevating the security level to MARSEC Level 2 twice a year each for 21 days will cost vessel owners and operators approximately $235 million annually.

We estimate that every regulated facility will have a Facility Security Officer assigned to it. We also estimate that there will also be a key person that can assist with security duties during MARSEC Level 2 at each facility. We assume that both Facility Security Officers and key personnel will work 12 hours a day (8 hours of regular time, 4 hours of overtime). For facilities that have to acquire security personnel for MARSEC Level 1, we assumed

that during MARSEC Level 2 the number security guards would double for this limited time. For the facilities for which we did not assume any additional guards at MARSEC Level 1, we assumed that during MARSEC Level 2 these would have to acquire a minimal number of security guards. Given these assumptions, we estimate that elevating the security level to MARSEC Level 2 twice a year each for 21 days will cost facility owners and operators approximately $424 million annually.

We estimate that elevating the security level to MARSEC Level 2 twice a year each for 21 days will cost the regulated OCS facility owners and operators approximately $4 million annually. This cost is primarily due to increased cost for OCS Facility Security Officers and available key security personnel.

Other costs that we did not attempt to quantify include possible operational restrictions such as limiting cargo operations to daylight hours or greatly limiting access to facilities or vessels.

MARSEC Level 3 will involve significant restriction of maritime operations that could result in the temporary closure of individual facilities, ports, and waterways either in a region of the U.S. or the entire nation. Depending on the nature of the specific threat, this

highest level of maritime security may have a considerable impact on the stakeholders in the affected ports or maritime areas. The ability to estimate the costs to business and government for even a short period at MARSEC Level 3 is virtually impossible with any level of accuracy or analytical confidence due to the infinite range of threats and scenarios that could trigger MARSEC Level 3.

The length and the duration of the increased security level to MARSEC Level 3 will be entirely dependent on the intelligence received and the scope of transportation security incidents or disasters that have already occurred or are imminent. While we can reasonably expect MARSEC Level 3 to increase the direct costs to businesses attributable to increased personnel or modified operations, we believe the indirect costs to society of the "ripple effects" associated with sustained port closures would greatly outweigh the direct costs to individual businesses.

The U.S. Marine Transportation System.

The cost of MARSEC Level 3 can best be appreciated by the benefits of the U.S. MTS to the economy. Maritime commerce is the lifeblood of the modern U.S. trade-based economy, touching virtually every sector of our daily business and personal activities.

Annually, the U.S. MTS contributes significant benefits to the economy. More than 95 percent of all overseas trade that enters or exits this country moves by ship, including 9 million barrels of oil a day that heats homes and businesses and fuels our automobiles.[1] In addition, over $738 billion of goods are transported annually through U.S. ports and waterways.[2]

Other benefits include the water transportation and shipping industry that generates over $24 billion in revenue and provides nearly $3 billion of payrolls.[3] The annual economic impact of cruise lines, passengers, and their suppliers is more than $11.6 billion in revenue and 176,000 in jobs for the U.S. economy.[1] Our national defense is also dependent on the MTS. Approximately 90 percent of all equipment and supplies for Desert Storm were shipped from strategic ports via our inland and coastal waterways.[1]

The Ripple Effect of Port Closures on the U.S. Economy

We could expect not just the immediate effects of port and waterway closures on waterborne commerce as described above, but also serious "ripple effects" for the entire U.S. economy that could last for months or more, including

---

[1] See MTS Fact Sheet available at www.dot.gov/mts/fact sheet.htm.
[2] See 2000 Exports and Imports by U.S. Customs District and Port available at www.marad.dot.gov/statististcs/usfwts/.

delayed commerce, decreased productivity, price increases, increased unemployment, unstable financial markets worldwide, and economic recession.

To appreciate the impact, we can examine one sector of the economy: agriculture. Many farm exports are just-in-time commodities, such as cotton shipped to Japan, South Korea, Indonesia, and Taiwan. Asian textile mills receive cotton on a just-in-time basis because these mills do not have warehousing capabilities. A port shutdown may cause U.S. cotton wholesalers to lose markets, as textile producers find suppliers from other nations. U.S. wholesalers would lose sales until shipping is restored.

Another example is the auto industry. A recent shutdown of West Coast ports due to a labor dispute caused an automobile manufacturer to delay production because it was not receiving parts to make its cars. We can see that a port shutdown can create a domino effect, from stalling the distribution of materials to causing stoppages and delays in production to triggering job losses, higher consumer prices, and limited selection.

The macroeconomic effects of the recent shutdown of West Coast ports, while not in response to a security

---

[3] U.S. Census Bureau, 1997 Economic Census, Transportation and Warehousing-Subject Series.

threat, are a good example of the economic costs that we could experience when a threat would necessitate broad-based port closures. The cost estimates of this 11-day interruption in cargo flow and closure of 29 West Coast ports have ranged between $140 million to $2 billion a day, but are obviously high enough to cause significant losses to the U.S. economy.[4]

Another proxy for the estimated costs to society of nationwide port closures and the consequential impact on the U.S. supply chain can be seen by a recent war game played by businesses and government agencies.[5] In that recent war game, a terrorist threat caused 2 major ports to close for 3 days, and then caused a nationwide port closure for an additional 9 days. This closure spanned only 12 days, but resulted in a delay of approximately 3 months to clear the resulting containerized cargo backlog. The economic costs of the closings attributable to manufacturing slowdowns and halts in production, lost

---

[4] See *Lost Earnings Due to West Coast Port Shutdown-Preliminary Estimate*, Patrick Anderson, October 7, 2002, available at http://www.AndersonEconomicGroup.com; *An Assessment of the Impact of West Coast Container Operations and the Potential Impacts of an Interruption of Port Operations, 2000*, Martin Associates, October 23, 2001, available from the Pacific Maritime Association. These two studies were widely quoted by most U.S. news services including Sam Zuckerman, *San Francisco Chronicle*, October 2002.

[5] The war game simulation was designed and sponsored by Booz Allen Hamilton and The Conference Board, details available at http://www.boozallen.com/.

sales, and spoilage was estimated at approximately be $58 billion. The simulation gauged how participants would respond to an attack and the ensuing economic consequences. Furthermore, a well-coordinated direct attack of multiple U.S. ports could shutdown the world economy by effectively halting international trade flows to and from the U.S. market--the largest market for goods and services in the world.

We believe that the cost to the national economy of a port shutdown due to extreme security threats, while not insignificant, would be relatively small if it only persisted for a few days and involved very few ports. However, if the interruption in cargo flows would persist much longer than the 11-day shutdown recently experienced on the West Coast, the economic loss is estimated to geometrically increase (double) every additional 10 days the ports were closed.[6] At a certain point, companies would start declaring bankruptcies, people would be laid off indefinitely, and the prices of goods would increase. This effect would continue and intensify until alternate economic activities took place, such as the unemployed finding less desirable jobs or companies finding secondary

[6] See Anderson.

lines of operations and suppliers. Regardless, the economic hardship suffered by industry, labor, and the loss of public welfare due to a sustained nationwide port shutdown may have as significant an effect on the U.S. as the act of terror itself.

Benefit Assessment

Why We Measured Benefits Using The N-RAT.

A team of experts considered the benefits of various security measures that will be implemented and used the N-RAT to estimate the reduction in risk associated with these security measures. Before the results of this assessment are discussed, it is helpful to understand why the Coast Guard chose this methodology to measure regulatory benefits.

Traditionally, the Coast Guard's regulations intended to decrease marine-related casualties, which in turn reduced number of injuries, fatalities, and pollution (primarily oil) spilled into the marine environment. These sorts of safety and environmental benefits could be estimated with some degree of accuracy; the well-documented and detailed history of maritime incidents provides a solid foundation to estimate the "costs to society" that could be avoided through enhanced requirements. By reviewing incident trends over time and the costs to society imposed

by these incidents, the Coast Guard could determine if changes to the status quo were justified.

Consequently, our environmental protection and marine safety regulations were generally accompanied by estimates of reduced injuries, fatalities, and pollution attributable to a specific regulation. For example, the recently promulgated Final Rule titled Tank Level or Pressure Monitoring Devices (published September 17, 2002) [67 FR 5815] estimated a benefit to society of approximately 900 barrels of oil not spilled into the environment over the period of assessment, though the regulation was not expected to prevent injuries or fatalities.

Estimating the benefits of new security requirements, however, is more challenging. Incident causation probabilities, based on historic trends and analysis, can be estimated in a manner that terrorist activities cannot. Currently, we believe it is virtually impossible to estimate benefits for security regulations in the way benefits are estimated for non-security regulations. We do not believe we can state with any degree of certainty that a specific security regulation would save a number or a range of fatalities, as no viable baseline exists from which to project these benefits. We realize though, that the burden on the regulated public of bearing the costs of

new security regulations will be high, and we must balance the benefits of these regulations with their associated costs. We must also consider the consequences of taking no action.

We do not assume the benefits of the interim rules automatically offset their costs simply because these rules are security related. By using RBDM, however, we have measured the relative risk reduction resulting from these security measures, permitting us to estimate the "value" these regulations will have. In considering the applicability of the interim rules, we have strived to apply requirements to those maritime entities that pose the greatest risk, and the N-RAT was an important and powerful tool in our Risk-Based Decision Making process. We believe that through better-informed judgments that came, in part, from the results of the N-RAT, we are appropriately balancing the benefits of the interim rules with their costs.

Results of the N-RAT Based Assessment.

The expert review and scoring process was complex and challenging. The fundamental principles of the N-RAT, however, are relatively simple to understand. For each applicable entity in the interim rules, we assigned an annual "baseline" risk score. We then considered the

requirements of the six interim rules described herein and assigned an annual post-regulation risk score. The benefits attributable to part 101 – General Provisions - were not considered separately because it is an overarching section for all the subparts. The benefits for part 101 are represented in each of the remaining security subparts. The difference between the baseline risk score and the post-regulation risk score is the quantified benefit of the remaining five interim rules.

Besides the complex procedure to assign risk scores to the applicable maritime entities, we were faced with the further complication that rules will have multiple benefits; thus, we have the potential to double-count the risk reduced. For example, if the owner or operator of a petroleum tanker enhances his vessel's security, this will also benefit the receiving facility where this vessel transfers its cargo. The reverse is also true: if the owner or operator of the facility enhances his facility's security, this will benefit the vessels that arrive there. We recognize that the interim rules are a "family" of rulemakings that will reinforce and support one another in their implementation. We must ensure, however, that risk reduction that is credited in one rulemaking is not also credited in another.

To avoid double-counting risk reduced, we first determined the "universe" of total benefits of *all* security measures recently implemented, about to be implemented, or planned for future rulemakings. Examples of other rules that were considered in the "universal" risk points are the Coast Guard's Notice of Arrival (96-Hour Rule), Custom's rulemaking regarding cargo manifests (24-Hour Rule), and a future rulemaking for transportation security cards. We then apportioned the total benefits to specific regulations. By approaching the benefits assessment in this manner, we were able to address the limitations of the N-RAT. The threat, vulnerability, and consequence scores are whole numbers between 1 and 5. The N-RAT did not allow us to score a relatively minor security initiative only 0.1 or 0.5 of a risk point, even though the initiative contributes to risk reduction. When we considered the rules as a group, however, security initiatives that could not be scored individually due to the limited granularity of the N-RAT can be scored when considered with the rest of the rules because of their cumulative risk reduction benefits.

Once we determined the total risk reduction benefits of the all the applicable rules, we "apportioned" the total risk points back to each individual regulation. We avoided

double-counting benefits among the rulemakings as each risk point was counted only once. While there was subjectivity in this apportionment of risk points back to the individual rulemakings, we believe this methodology's strength of allowing a systematic quantification of risk reduction for each regulation outweighs its subjectivity.

Results of the N-RAT.

We determined annual risk points reduced for each of the six interim rules using the N-RAT. Table 7 presents the annual risk points reduced by the rules. As shown, the interim rule for vessel security plans reduces the most risk points annually. The interim rule for AIS reduces the least.

Table 7. Annual Risk Points Reduced by the interim rules.

Maritime Entity	Annual Risk Points Reduced by Rulemaking				
	Vessel Security Plans	Facility Security Plans	OCS Facility Security Plans	AMS Plans	AIS
Vessels	778,633	3,385	3,385	3,385	1,448
Facilities	2,025	469,686	-	2,025	-
OCS Facilities	41	-	9,903	-	-
Port Areas	587	587	-	129,792	105
Total	781,285	473,659	13,288	135,202	1,553

Once we determined the annual risk points reduced, we discounted these estimates to their PV (7 percent discount rate, 2003-2012) so that they could be compared to the costs. We presented the cost effectiveness, or dollars per

risk point reduced, in two ways: first, we compared first-year cost to first-year benefit, because first-year cost is the highest in our assessment as companies develop security plans and purchase equipment. Second, we compared the 10-year PV cost to the 10-year PV benefit. The results of our assessment are presented in Table 8.

Table 8. First-Year and 10-Year PV Cost and Benefit of the interim rules.

Item	Interim Rule				
	Vessel Security Plans	Facility Security Plans	OCS Facility Security Plans	AMS Plans	AIS*
First-Year Cost (millions)	$218	$1,125	$3	$120	$41
First-Year Benefit	781,285	473,659	13,288	135,202	1,553
First-Year Cost Effectiveness ($/Risk Point Reduced)	$279	$2,375	$205	$890	$26,391
10-Year PV Cost (millions)	$1,368	$5,399	$37	$477	$42
10-Year PV Benefit	5,871,540	3,559,655	99,863	1,016,074	11,671
10-Year PV Cost Effectiveness ($/Risk Point Reduced)	$233	$1,517	$368	$469	$3,624

*Cost less monetized safety benefit.

As shown, the rulemaking for vessel security plans is the most cost effective. This is due to the nature of the security measures we expect vessels will have to take to ensure compliance as well as the level of risk that is reduced by those measures. Facility security plans are less cost effective because they incur higher costs for capital purchases (such as gates and fences) and require

more labor (such as security guards) to ensure security. OCS Facility and AMS Plans are almost equally cost effective; the entities these rules cover do not incur the highest expenses for capital equipment, but on this relative scale, they do not receive higher risk reduction in the N-RAT, either. The AIS rulemaking is the least cost effective, though it is important to remember that AIS provides increased maritime domain awareness and navigation safety, which is not robustly captured using the N-RAT.

Small Entities

Under the Regulatory Flexibility Act (5 U.S.C. 601-612), we have considered whether these interim rules would have a significant economic impact on a substantial number of small entities. The term "small entities" comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. These interim rules do not require a general notice of proposed rulemaking and, therefore, are exempt from the requirements of the Regulatory Flexibility Act.

Although these interim rules are exempt, we have reviewed each rule for potential economic impacts on small entities. We found that the facilities, vessels, and AIS

rules may have a significant impact on a substantial number of small entities. However, we did certify no significant economic impact on a substantial number of small entities for the Area Maritime Security and OCS facility security rules. Additional information on small entity impacts is available in the Regulatory Assessment or Cost Assessment for each interim rule in their associated docket, where indicated in the ADDRESSES section for each interim rule.

Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996 (Public Law 104-121), we want to assist small entities in understanding these rules so that they can better evaluate the effects on them and participate in the rulemaking. If these rules affect your small business, organization, or governmental jurisdiction and you have questions concerning their provisions or options for compliance, please consult CDR Suzanne Englebert, G-M-1 by telephone 202-267-1103, toll-free telephone 1-800-842-8740 ext. 7-1103, or by electronic mail msregs@comdt.uscg.mil.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the

Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1-888-REG-FAIR (1-888-734-3247).

Collection of Information

The interim rules published in today's Federal Register contain collection of information requirements under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). As defined in 5 CFR 1320.3(c), "collection of information" comprises reporting, recordkeeping, monitoring, posting, labeling, and other, similar actions. The rules modify two existing OMB-approved collections--1625-0100 [formerly 2115-0557] and 1625-0077 [formerly 2115-0622]. Details of the revision to 1625-0100 can be found in the "Vessel Security" [USCG-2003-14749] interim rule published elsewhere in today's Federal Register. A summary of the revised collection 1625-0077 follows.

TITLE: Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements.

OMB CONTROL NUMBER: 1625-0077

SUMMARY OF THE COLLECTION OF INFORMATION: The Coast Guard requires security plans and communication procedures

for U.S. ports and maritime areas as detailed in the interim rules. These rules provide a framework to ensure adequate security planning, drilling, and communication procedures for Ports, Vessels, Facilities, and OCS Facilities.

NEED FOR INFORMATION: The primary need for information would be to determine if stakeholders are in compliance with security standards.

PROPOSED USE OF INFORMATION: This information can help to determine appropriate security measures for the affected population. This information also can help determine, in the case of a transportation security incident, whether failure to meet these regulations contributed to the transportation security incident.

DESCRIPTION OF THE RESPONDENTS: This rule will affect owners, operators, and personnel operating in the U.S. Marine Transportation System. The respondents are regulated public and private stakeholders as detailed in the interim rules.

NUMBER OF RESPONDENTS: 16,607 total respondents for the interim rules.

FREQUENCY OF RESPONSE: Varies as specified in each interim rule. Security assessments and security plans are submitted for approval initially, and reviewed annually.

After the first year, drills generally occur at various schedules. All frequencies are at the discretion of the COTP. Depending on the port or maritime area, there may be additional requirements and reporting frequencies.

BURDEN OF RESPONSE: Varies per each type of regulated population in the interim rules.

ESTIMATE OF TOTAL ANNUAL BURDEN: The existing OMB-approved collection total annual burden is 1,811 hours. These interim rules are a program change that will increase the total annual burden. The new estimated total collection burden is indicated in the table below.

Table 9. Summary of Initial and Annual Burden Hours and Costs.

	BURDEN (hours)	
	Initial	Annual
Port Security (AMS)	1,203,200	488,800
Vessel Security	135,269	11,700
Facility Security	528,240	608,187
OCS Facility Security	3,200	160
SUBTOTAL	1,869,909	1,108,847
Pre 9/11 Security	3,549*	3,549
TOTAL	1,873,458	1,112,396

*As pre-9/11/01 security requirements are existing regulations, they are included in both initial and annual burden calculations (Note burden revised from year 2000 Estimate)

As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)), we have submitted a copy of the interim rules to the OMB for its review of the collection of information. Due to the circumstances surrounding this temporary rule, we asked for "emergency processing" of our request. We received OMB approval for these collections of information on June 16, 2003. They are valid until December 31, 2003.

We ask for public comment on the collection of information to help us determine how useful the information is; whether it can help us perform our functions better; whether it is readily available elsewhere; how accurate our estimate of the burden of collection is; how valid our methods for determining burden are; how we can improve the quality, usefulness, and clarity of the information; and how we can minimize the burden of collection.

If you submit comments on the collection of information, submit them both to OMB and to the Docket Management Facility where indicated under ADDRESSES, by the date under DATES.

You need not respond to a collection of information unless it displays a currently valid control number from OMB. We received OMB approval for these collections of

information on June 16, 2003. They are valid until December 31, 2003.

Federalism

Executive Order 13132 requires USCG to develop an accountable process to ensure "meaningful and timely input by State and local officials in the development of regulatory policies that have federalism implications." "Policies that have federalism implications" is defined in the Executive Order to include regulations that have "substantial direct effects on the States, on the relationship between the national government and the States, or on the distribution of power and responsibilities among the various levels of government." Under the Executive Order, USCG may construe a Federal statute to preempt State law only where, among other things, the exercise of State authority conflicts with the exercise of Federal authority under the Federal statute.

This action has been analyzed in accordance with the principles and criteria in the Executive Order, and it has been determined that this interim rule does have Federalism implications or a substantial direct effect on the States. This rulemaking requires those States which own or operate vessels or facilities that may be involved in a transportation security incident to conduct vulnerability

assessments of their vessels and facilities and to develop security plans for their protection. These plans must contain measures that will be implemented at each of the three MARSEC Levels, and must be reviewed and approved by the Coast Guard.

Additionally, the Coast Guard has reviewed the MTSA with a view to whether we may construe it as non-preemptive of State authority over the same subject matter. We have determined that it would be inconsistent with the federalism principles stated in the Executive Order to construe the MTSA as not preempting State regulations which conflict with the regulations in this rulemaking. This is because owners or operators of facilities and vessels that are subject to the requirements for conducting vulnerability assessments, planning to secure their facilities and vessels against threats revealed by those assessments and complying with the standards, both performance and specific construction, design, equipment and operating requirements, must have one uniform, national standard which they must meet. Vessels and shipping companies, particularly, would be confronted with an unreasonable burden if they had to comply with varying requirements as they moved from State to State. Therefore, we believe that the federalism principles

enunciated by the Supreme Court in U.S. v. Locke, 529 U.S. 89 (2000) regarding field preemption of certain State vessel safety, equipment and operating requirements extends equally to this rulemaking, especially regarding the longstanding history of significant Coast Guard maritime security regulation and control of vessels for security purposes. But, the same considerations apply to facilities, at least insofar as a State law or regulation applicable to the same subject for the purpose of protecting the security of the facility would conflict with a federal regulation, i.e. it would either actually conflict or would frustrate an over-riding federal need for uniformity.

Finally, it is important to note that the regulations implemented by this rulemaking bear on national and international commerce where there is no constitutional presumption of concurrent State regulation. Many aspects of these regulations are based on the U.S. international treaty obligations regarding vessel and port facility security contained in the International Convention for the SOLAS, 1974 and the complementary ISPS Code. These international obligations reinforce the need for uniformity regarding maritime commerce.

Notwithstanding the foregoing preemption determinations and findings, the Coast Guard has consulted extensively with appropriate State officials, as well as private stakeholders during the development of this rule. Specifically, we have held seven public meetings across the country with invitation letters to all State homeland security representatives. Many State representatives attended these meetings and submitted comments to the public notice docket that we have considered for these interim rules. The State comments ranged from State Boating Law Administrators concerns about recreational boating impacts and security for smaller marinas to State security representatives voicing concern about alignment with their State maritime security requirements. We also presented the SOLAS Amendments and ISPS Code, parts A and B, in the public notice and requested comments from the State homeland security advisors at a National Governors Association meeting on March 14, 2003. We encourage States to send in comments specifically on this Federalism analysis.

Unfunded Mandates Reform Act

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) requires Federal agencies to assess the effects of their discretionary regulatory actions. In particular,

the Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of $100,000,000 or more in any one year. This rule is exempted from assessing the effects of the regulatory action as required by the Act because it is necessary for the national security of the U.S. (2 U.S.C. 1503(5)).

Taking of Private Property

This rule will not effect a taking of private property or otherwise have taking implications under Executive Order 12630, Governmental Actions and Interference with Constitutionally Protected Property Rights.

Civil Justice Reform

This rule meets applicable standards in sections 3(a) and 3(b)(2) of Executive Order 12988, Civil Justice Reform, to minimize litigation, eliminate ambiguity, and reduce burden.

Protection of Children

We have analyzed this rule under Executive Order 13045, Protection of Children from Environmental Health Risks and Safety Risks. While this rule is an economically significant rule, it does not create an environmental risk to health or risk to safety that may disproportionately affect children.

Indian Tribal Governments

This rule does not have tribal implications under Executive Order 13175, Consultation and Coordination with Indian Tribal Governments, because it does not have a substantial disproportionate effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes. We would appreciate any comments, however, if you disagree with this conclusion.

Energy Effects

We have analyzed this rule under Executive Order 13211, Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use. We have determined that it is not a "significant energy action" under that order. Although it is a "significant regulatory action" under Executive Order 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy. Additionally, the Administrator of the Office of Information and Regulatory Affairs has not designated it as a significant energy action. Therefore, it does not require a Statement of Energy Effects under Executive Order 13211.

This rule has a positive effect on the supply, distribution, and use of energy. The rule provides for security assessments, plans, procedures, and standards, which will prove beneficial for the supply, distribution, and use of energy at increased levels of maritime security.

Environment

We have considered the environmental impact of this rule and concluded that under figure 2-1, paragraph (34)(a), (34)(c), (34)(d), and (34)(e) of Commandant Instruction M16475.lD, this rule is categorically excluded from further environmental documentation. A "Categorical Exclusion Determination" is available in the docket where indicated under ADDRESSES or SUPPLEMENTARY INFORMATION.

This final rule concerns security assessments, plans, training, security positions, and organizations along with vessel equipment requirements that will contribute to a higher level of marine safety and security for U.S. ports. A "Categorical Exclusion Determination" is available in the docket where indicated under ADDRESSES or SUPPLEMENTARY INFORMATION.

This rulemaking will not significantly impact the coastal zone. Further, the rulemaking and the execution of this rule will be done in conjunction with appropriate State coastal authorities. The Coast Guard will,

therefore, comply with the requirements of the Coastal Zone Management Act while furthering its intent to protect the coastal zone.

Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits federal agencies from engaging in any standards or related activities that create unnecessary obstacles to the foreign commerce of the U.S. Legitimate domestic objectives, such as safety and security, are not considered unnecessary obstacles. The Act also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. We have assessed the potential effect of this regulation, and have determined that it would likely create obstacles to the foreign commerce of the U.S.. However, because these regulations are being put in place in order to further a legitimate domestic objective, namely to increase the security of the U.S., any obstacles created by the regulation are not considered unnecessary obstacles.

List of Subjects

33 CFR Part 101

Facilities, Harbors, Incorporation by reference, Maritime security, Ports, Security assessments, Security

plans, Reporting and recordkeeping requirements, Vessels, Waterways.

33 CFR Part 102

Maritime security.

For the reasons discussed in the preamble, the Coast Guard is adding subchapter H consisting of part 101 and reserved part 102 to 33 CFR chapter I to read as follows:

Subchapter H—Maritime Security

PART 101—GENERAL PROVISIONS

Subpart A—General

Sec.

Subpart B—Maritime Security (MARSEC) Levels

Authority: 33 U.S.C. 1231, 1226; 46 U.S.C. Chapter 701; 50 U.S.C. 191, 192; E.O. 12656; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 0170.

PART 102—NATIONAL MARITIME TRANSPORTATION SECURITY

[RESERVED]

PART 101—GENERAL PROVISIONS

Subpart A—General

§ 101.100 Purpose.

(a) The purpose of this part is:

(1) To implement portions of the maritime security regime required by the Maritime Transportation Security Act of 2002, as codified in 46 U.S.C. Chapter 701;

(2) To align, where appropriate, the requirements of domestic maritime security regulations with the international maritime security standards in the International Convention for the Safety of Life at Sea, 1974 (SOLAS Chapter XI-2) and the International Code for the Security of Ships and of Port Facilities, parts A and B, adopted on 12 December 2002; and

(3) To ensure security arrangements are as compatible as possible for vessels trading internationally.

(b) For those maritime elements of the national transportation system where international standards do not directly apply, the requirements in this subchapter emphasize cooperation and coordination with local port community stakeholders, and are based on existing domestic standards, as well as established industry security practices.

§ 101.105 Definitions.

Unless otherwise specified, as used in this subchapter:

Alternative Security Program means a third-party or industry organization developed standard that the Commandant has determined provides an equivalent level of security to that established by this subchapter.

Area Commander means the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard Area as described in 33 CFR part 3.

Area Maritime Security (AMS) Assessment means an analysis that examines and evaluates the infrastructure and operations of a port taking into account possible threats, vulnerabilities, and existing protective measures, procedures and operations.

Area Maritime Security (AMS) Committee means the committee established pursuant to 46 U.S.C. 70112(a)(2)(A). This committee can be the Port Security Committee established pursuant to Navigation and Vessel Inspection Circular (NVIC) 09-02, available from the cognizant Captain of the Port (COTP) or at http://www.uscg.mil/hq/g-m/nvic.

Area Maritime Security (AMS) Plan means the plan developed pursuant to 46 U.S.C. 70103(b). This plan may be the Port Security plan developed pursuant to NVIC 09-02

provided it meets the requirements of part 103 of this subchapter.

Area of Responsibility (AOR) means a Coast Guard area, district, marine inspection zone or COTP zone described in 33 CFR part 3.

Audit means an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third-party, intended to identify deficiencies, non-conformities and/or inadequacies that would render the assessment or plan insufficient.

Barge means a non-self-propelled vessel (46 CFR 24.10-1)

Barge fleeting facility means a commercial area, permitted by the Army Corps of Engineers, as provided in 33 CFR part 322, the purpose of which is for the making up, breaking down, or staging of barge tows.

Bulk or in bulk means a commodity that is loaded or carried on board a vessel without containers or labels, and that is received and handled without mark or count.

Bunkers means a vessel's fuel supply.

Captain of the Port (COTP) means the local officer exercising authority for the COTP zones described in 33 CFR part 3. The COTP is the Federal Maritime Security

Coordinator described in 46 U.S.C. 70103(a)(2)(G) and also the Port Facility Security Officer as described in the ISPS Code, part A.

Cargo means any goods, wares, or merchandise carried, or to be carried, for consideration, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person interested in the vessel, facility, or OCS facility.

Certain Dangerous Cargo (CDC) means the same as defined in 33 CFR 160.203.

Commandant means the Commandant of the U.S. Coast Guard.

Company means any person or entity that owns any facility, vessel, or OCS facility subject to the requirements of this subchapter, or has assumed the responsibility for operation of any facility, vessel, or OCS facility subject to the requirements of this subchapter, including the duties and responsibilities imposed by this subchapter.

Company Security Officer (CSO) means the person designated by the Company as responsible for the security of the vessel or OSC facility, including implementation and maintenance of the vessel or OSC facility security plan,

and for liaison with their respective vessel or facility security officer and the COTP.

Contracting Government means any government of a nation that is a signatory to SOLAS, other than the U.S.

Cruise ship means any vessel over 100 gross register tons, carrying more than 12 passengers for hire which makes voyages lasting more than 24 hours, of which any part is on the high seas. Passengers from cruise ships are embarked or disembarked in the U.S. or its territories. Cruise ships do not include ferries that hold Coast Guard Certificates of Inspection endorsed for "Lakes, Bays, and Sounds", that transit international waters for only short periods of time on frequent schedules.

Dangerous substances or devices means any material, substance, or item that may cause damage or injury to any person, vessel, facility, harbor, port, or waters subject to the jurisdiction of the U.S. and that:

(1) Is unlawful to possess under applicable Federal, State, or local law;

(2) That has not been approved for entry onto the vessel, facility, or OCS facility by the owner or operator of the vessel, facility, or OCS facility; or

(3) Has not been approved for entry onto a public area or property in a port by the government or property

management official with jurisdictional responsibility of that area.

Declaration of Security (DoS) means an agreement executed between the responsible Vessel and Facility Security Officer, or between Vessel Security Officers in the case of a vessel-to-vessel interface, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel interface, respectively.

District Commander means the U.S. Coast Guard officer designated by the Commandant to command a Coast Guard District described in 33 CFR part 3.

Drill means a training event that tests at least one component of the AMS, vessel, or facility security plan and is used to maintain a high level of security readiness.

Exercise means a comprehensive training event that involves several of the functional elements of the AMS, vessel, or facility security plan and tests communications, coordination, resource availability, and response.

Facility means any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the U.S. and used, operated, or

maintained by a public or private entity, including any contiguous or adjoining property under common ownership or operation.

Facility Security Assessment (FSA) means an analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.

Facility Security Officer (FSO) means the person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the COTP and Company and Vessel Security Officers.

Facility Security Plan (FSP) means the plan developed to ensure the application of security measures designed to protect the facility and its servicing vessels or those vessels interfacing with the facility, their cargoes, and persons on board at the respective MARSEC Levels.

Ferry means a vessel which is limited in its use to the carriage of deck passengers or vehicles or both, operates on a short run on a frequent schedule between two or more points over the most direct water route, other than in ocean or coastwise service.

Foreign vessel means a vessel of foreign registry or a vessel operated under the authority of a country, except the U.S., that is engaged in commerce.

Gross register tons (GRT) means the gross ton measurement of the vessel under 46 U.S.C. chapter 145, Regulatory Measurement. For a vessel measured under only 46 U.S.C. chapter 143, Convention Measurement, the vessel's gross tonnage, ITC is used to apply all thresholds expressed in terms of gross register tons.

Gross tonnage, ITC (GT ITC) means the gross tonnage measurement of the vessel under 46 U.S.C. chapter 143, Convention Measurement. Under international conventions, this parameter may be referred to as "gross tonnage (GT)."

Hazardous materials means hazardous materials subject to regulation under 46 CFR parts 148, 150, 151, 153, or 154, or 49 CFR parts 171 through 180.

Infrastructure means facilities, structures, systems, assets, or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health or safety of the port.

International voyage means a voyage between a country to which SOLAS applies and a port outside that country. A

country, as used in this definition, includes every territory for the internal relations of which a contracting government to the convention is responsible or for which the United Nations is the administering authority. For the U.S., the term "territory" includes the Commonwealth of Puerto Rico, all possessions of the United States, and all lands held by the U.S. under a protectorate or mandate. For the purposes of this subchapter, vessels are considered as being on an "international voyage" when solely navigating the Great Lakes and the St. Lawrence River as far east as a straight line drawn from Cap des Rosiers to West Point, Anticosti Island and, on the north side of Anticosti Island, the 63rd meridian.

ISPS Code means the International Ship and Port Facility Security Code, as incorporated into SOLAS.

Maritime Security (MARSEC) Directive means an instruction issued by the Commandant, or his/her delegee, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.

Maritime Security (MARSEC) Level means the level set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and

infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

MARSEC Level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

MARSEC Level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.

MARSEC Level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

Master means the holder of a valid license that authorizes the individual to serve as a Master, operator, or person in charge of the rated vessel. For the purposes of this subchapter, Master also includes the Person in Charge of a MODU, and the operator of an uninspected towing vessel.

OCS Facility means any artificial island, installation, or other complex of one or more structures permanently or temporarily attached to the subsoil or seabed of the OCS, erected for the purpose of exploring

for, developing or producing oil, natural gas or mineral resources. This definition includes all mobile offshore drilling units (MODUs) not covered under part 104 of this subchapter, when attached to the subsoil or seabed of offshore locations, but does not include deepwater ports, as defined by 33 U.S.C. 1502, or pipelines.

Operator, Uninspected Towing Vessel means an individual who holds a license described in 46 CFR 15.805(a)(5) or 46 CFR 15.810(d).

Owner or operator means any person or entity that maintains operational control over any facility, vessel, or OCS facility subject to the requirements of this subchapter.

Passenger vessel means

(1) On an international voyage, a vessel carrying more than 12 passengers; and

(2) On other than an international voyage:

(i) A vessel of at least 100 gross register tons carrying more than 12 passengers, including at least one passenger-for-hire;

(ii) A vessel of less than 100 gross register tons carrying more than 6 passengers, including at least one passenger-for-hire;

(iii) A vessel that is chartered and carrying more than 12 passengers;

(iv) A submersible vessel that is carrying at least one passenger-for-hire; or

(v) A wing-in-ground craft, regardless of tonnage, that is carrying at least one passenger-for-hire.

Passenger-for-hire means a passenger for whom consideration is contributed as a condition of carriage on the vessel, whether directly or indirectly flowing to the owner, charterer, operator, agent, or any other person having an interest in the vessel.

Registered length means the registered length as defined in 46 CFR part 69.

Restricted areas mean the infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection. The entire facility maybe designated the restricted area, as long as the entire facility is provided the appropriate level of security.

Review and approval means the process whereby Coast Guard officials evaluate a plan or proposal to determine if it complies with this subchapter and/or provides an equivalent level of security.

Screening means a reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present.

Security sweep means a walkthrough to visually inspect unrestricted areas to identify unattended packages, briefcases, or luggage and determine that all restricted areas are secure.

Security system means a device or multiple devices designed, installed and operated to monitor, detect, observe or communicate about activity that may pose a security threat in a location or locations on a vessel or facility.

Sensitive security information (SSI) means information within the scope of 49 CFR part 1520.

SOLAS means the International Convention for the Safety of Life at Sea Convention, 1974, as amended.

Survey means an on-scene examination and evaluation of the physical characteristics of a vessel or facility, and its security systems, processes, procedures, and personnel.

Transportation security incident (TSI) means a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.

Unaccompanied baggage means any baggage, including personal effects, which are not with the passenger, crewmember or any other person at the point of inspection or screening prior to boarding the vessel.

Vessel-to-facility interface means the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, goods or the provisions of facility services to or from the vessel.

Vessel-to-port interface means the interaction that occurs when a vessel is directly and immediately affected by actions involving the movement of persons, goods or the provisions of port services to or from the vessel.

Vessel Security Assessment (VSA) means an analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities,

consequences, and existing protective measures, procedures and operations.

Vessel Security Plan (VSP) means the plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with, the vessel's cargoes, and persons on board at the respective MARSEC Levels.

Vessel Security Officer (VSO) means the person onboard the vessel, accountable to the Master, designated by the Company as responsible for security of the vessel, including implementation and maintenance of the Vessel Security Plan, and for liaison with the Facility Security Officer and the vessel's Company Security Officer.

Vessel stores means

(1) Materials that are on board a vessel for the upkeep, maintenance, safety, operation or navigation of the vessel; and

(2) Materials for the safety or comfort of the vessel's passengers or crew, including any provisions for the vessel's passengers or crew.

Vessel-to-vessel activity means any activity not related to a facility or port that involves the transfer of goods or persons from one vessel to another.

Waters subject to the jurisdiction of the U.S., for purposes of this subchapter, means the navigable waters of the U.S., as defined in 46 U.S.C. 2101(17a); the Exclusive Economic Zone in respect to the living and non-living resources therein; and in respect to facilities located on the Outer Continental Shelf of the U.S., the waters superajacent thereto.

§ 101.110 Applicability.

Unless otherwise specified, this subchapter applies to vessels, structures, and facilities of any kind, located under, in, on, or adjacent to waters subject the jurisdiction of the U.S.

§ 101.115 Incorporation by reference.

(a) Certain material is incorporated by reference into this subchapter with the approval of the Director of the Federal Register under 5 U.S.C. 552(a) and 1 CFR part 51. To enforce any edition other than that specified in paragraph (b) of this section, the Coast Guard must publish notice of change in the Federal Register and the material must be available to the public. All approved material is on file at the Office of the Federal Register, 800 North Capitol Street, NW, Suite 700, Washington, DC, and at the Office of the Coast Guard Port Security Directorate (G-MP), Coast Guard Headquarters, 2100 Second Street, SW,

Washington, DC 20593-0001, and is available from the sources indicated in paragraph (b) of this section.

(b) The materials approved for incorporation by reference in this subchapter are as follows:

International Maritime Organization (IMO)

Publication Section, 4 Albert Embankment, London SE1 7SR, United Kingdom.

Conference resolution 1, Adoption of amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974, and amendments to Chapter XI of SOLAS 1974, adopted December 12, 2002, (SOLAS Chapter XI-1 or SOLAS Chapter XI-2) 101.120; 101.310; 101.410; 101.505; 104.105; 104.115; 104.120; 104.297; 104.400

Conference resolution 2, Adoption of the International Code for the Security of

Ships and of Port Facilities, parts A and B, adopted on December 12, 2002 (ISPS Code). 101.410; 101.505; 104.105; 104.115; 104.120; 104.297; 104.400

§ 101.120 Alternatives.

(a) Alternative Security Agreements.

(1) The U.S. may conclude in writing, as provided in SOLAS Chapter XI-2, Regulation 11 (Incorporated by reference, see § 101.115), a bilateral or multilateral agreements with other Contracting Governments to SOLAS on Alternative Security Arrangements covering short international voyages on fixed routes between facilities subject to the jurisdiction of the U.S. and facilities in the territories of those Contracting Governments.

(2) As further provided in SOLAS Chapter XI-2, Regulation 11, a vessel covered by such an agreement shall not conduct any vessel-to-vessel activity with any vessel not covered by the agreement.

(b) Alternative Security Programs.--

(1) Owners and operators of vessels and facilities required to have security plans under part 104, 105, or 106 of this subchapter, other than vessels that engage on international voyages and facilities that serve only vessels on international voyages, may meet an Alternative Security Program that has been reviewed and approved by the Commandant (G-MP) as meeting the requirements of part 104, 105, or 106, as applicable.

(2) Owners or operators must implement an approved Alternative Security Program in its entirety to be deemed in compliance with either part 104, 105, or 106.

(3) Owners or operators who have implemented an Alternative Security Program must send a letter to the appropriate plan approval authority under part 104, 105, or 106 of this subchapter identifying which Alternative Security Program they have implemented, identifying those vessels or facilities that will implement the Alternative Security Program, and attesting that they are in full compliance therewith. A copy of this letter shall be retained on board the vessel or kept at the facility to which it pertains along with a copy of the Alternative Security Program.

(c) Approval of Alternative Security Programs. You must submit to the Commandant (G-MP) for review and

approval the Alternative Security Program and the following information to assess the adequacy of the proposed Alternative Security Program:

(1) A list of the vessel and facility type that the Alternative Security Program is intended to apply;

(2) A security assessment for the vessel or facility type;

(3) Explanation of how the Alternative Security Program addresses the requirements of parts 104, 105, or 106, as applicable; and

(4) Explanation of how owners and operators must implement the Alternative Security Program in its entirety, including performing an operational and vessel or facility specific assessment and verification of implementation.

(d) The Commandant (G-MP) will examine each submission for compliance with this part, and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions, or

(2) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

§ 101.125 Approved Alternative Security Programs.

[RESERVED]

§ 101.130 Equivalent security measures.

(a) For any measure required by part 104, 105, or 106 of this subchapter, the owner or operator may substitute an equivalent security measure that has been approved by the Commandant (G-MP) as meeting or exceeding the effectiveness of the required measure. The Commandant (G-MP) may require that the owner or operator provide data for use in assessing the effectiveness of the proposed equivalent security measure.

(b) Requests for approval of equivalent security measures should be made to the appropriate plan approval authority under parts 104, 105 or 106 of this subchapter.

Subpart B—Maritime Security (MARSEC) Levels

§ 101.200 MARSEC Levels.

(a) MARSEC Levels advise the maritime community and the public of the level of risk to the maritime elements of the national transportation system. Ports, under direction of the local COTP, will respond to changes in the MARSEC Level by implementing the measures specified in the AMS Plan. Similarly, vessels and facilities required to have security plans under part 104, 105, or 106 of this

subchapter shall implement the measures specified in their security plans for the applicable MARSEC Level.

(b) Unless otherwise directed, each port, vessel, and facility shall operate at MARSEC Level 1.

(c) The Commandant will set the MARSEC Level consistent with the equivalent Homeland Security Advisory System (HSAS) Threat Condition and that Threat Condition's scope of application. Notwithstanding the HSAS, the Commandant retains discretion to adjust the MARSEC Level when necessary to address any particular security concerns or circumstances related to the maritime elements of the national transportation system.

(d) The COTP may temporarily raise the MARSEC Level for the port, a specific marine operation within the port, or a specific industry within the port, when necessary to address an exigent circumstance immediately affecting the security of the maritime elements of the transportation system in his/her area of responsibility.

§ 101.205 Department of Homeland Security alignment.

The MARSEC Levels are aligned with the Department of Homeland Security's Homeland Security Advisory System (HSAS), established by Homeland Security Presidential Directive 3. Table 101.205, titled "Relation between HSAS and MARSEC Levels" in this section, shows this alignment.

Table 101.205 Relation Between HSAS and MARSEC Levels.

Homeland Security Advisory System (HSAS) Threat Condition		Equivalent Maritime Security (MARSEC) Level
Low Elevated Guarded	Green Blue Yellow	MARSEC Level 1
High	Orange	MARSEC Level 2
Severe	Red	MARSEC Level 3

Subpart C—Communication (Port — Facility — Vessel)

§ 101.300 Preparedness communications.

(a) Notification of MARSEC Level change. The COTP will communicate any changes in the MARSEC Levels through a local Broadcast Notice to Mariners, a Maritime Security Directive issued under section 101.405 of this part, or as detailed in the AMS Plan.

(b) Communication of threats. When the COTP is made aware of a threat that may cause a transportation security incident, the COTP will, when appropriate, communicate to the port stakeholders, vessels, and facilities in his or her AOR the following details:

(1) Geographic area potentially impacted by the probable threat;

(2) Any appropriate information identifying potential targets;

(3) Onset and expected duration of probable threat;

(4) Type of probable threat; and

(5) Required actions to minimize risk.

(c) Attainment.--

(1) Each owner or operator of a vessel or facility required to have a security plan under parts 104 or 105 of this subchapter affected by a change in the MARSEC Level must confirm to their local COTP the attainment of measures or actions described in their security plan and any other requirements imposed by the COTP that correspond with the MARSEC Level being imposed by the change.

(2) Each owner or operator of a facility required to have a security plan under part 106 of this subchapter affected by a change in the MARSEC Level must confirm to their cognizant District Commander the attainment of measures or actions described in their security plan and any other requirements imposed by the District Commander or COTP that correspond with the MARSEC Level being imposed by the change.

§ 101.305 Reporting.

(a) Notification of suspicious activities. An owner or operator required to have a security plan under part

104, 105, or 106 of this subchapter shall, without delay, report activities that may result in a transportation security incident to the National Response Center at the following toll free telephone: 1-800-424-8802, direct telephone: 202-267-2675, fax: 202-267-2165, TDD: 202-267-4477, or Email: lst-nrcinfo@comdt.uscg.mil.
Any other person or entity is also encouraged to report activities that may result in a transportation security incident to the National Response Center.

(b) Notification of breaches of security. An owner or operator required to have a security plan under parts 104, 105, or 106 of this subchapter shall, without delay, report breaches of security to the National Response Center via one of the means listed in paragraph (a) of this section.

(c) Notification of transportation security incident (TSI).

(1) Any owner or operator required to have a security plan under part 104 or 105 of this subchapter shall, without delay, report a TSI to their local COTP and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(2) Any owner or operator required to have a security plan under part 106 of this subchapter shall, without delay, report a TSI to their cognizant District Commander and immediately thereafter begin following the procedures set out in their security plan, which may include contacting the National Response Center via one of the means listed in paragraph (a) of this section.

(d) Callers to the National Response Center should be prepared to provide as much of the following information as possible:

(1) Their own name and contact information;

(2) The name and contact information of the suspicious or responsible party;

(3) The location of the incident, as specifically as possible; and

(4) The description of the incident or activity involved.

§ 101.310 Additional communication devices.

(a) Alert Systems. Alert systems, such as the ship security alert system required in SOLAS Chapter XI-2, Regulation 6 (Incorporated by reference, see § 101.115), may be used to augment communication and may be one of the communication methods listed in a vessel or facility

security plan under part 104, 105, or 106 of this subchapter.

(b) Automated Identification Systems (AIS). AIS may be used to augment communication, and may be one of the communication methods listed in a vessel security plan under part 104 of this subchapter. See 33 CFR part 164 for additional information on AIS device requirements.

Subpart D—Control Measures for Security

§ 101.400 Enforcement.

(a) The rules and regulations in this subchapter are enforced by the COTP under the supervision and general direction of the District Commander, Area Commander, and the Commandant. All authority and power vested in the COTP by the rules and regulations in this subchapter is also vested in, and may be exercised by, the District Commander, Area Commander, and the Commandant.

(b) The COTP, District Commander, Area Commander, or Commandant may assign the enforcement authority described in paragraph (a) of this section to any other officer or petty officer of the Coast Guard or other designees authorized by the Commandant.

(c) The provisions in this subchapter do not limit the powers conferred upon Coast Guard commissioned,

warrant, or petty officers by any other law or regulation, including but not limited to 33 CFR parts 6, 160, and 165.

§ 101.405 Maritime Security (MARSEC) Directives.

(a) (1) When the Coast Guard determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against the maritime elements of the national transportation system, the Coast Guard may issue a MARSEC Directive setting forth mandatory measures. Only the Commandant or his/her delegee may issue MARSEC Directives under this section. Prior to issuing a MARSEC Directive, the Commandant or his/her delegee will consult with those Federal agencies having an interest in the subject matter of that MARSEC Directive. All MARSEC Directives issued under this section shall be marked as sensitive security information (SSI) in accordance with 49 CFR part 1520.

(2) When a MARSEC Directive is issued, the Coast Guard will immediately publish a notice in the Federal Register, and affected owners and operators will need to go to their local COTP or cognizant District Commander to acquire a copy of the MARSEC Directive. COTPs and District Commanders will require the owner or operator to prove that they have a "need to know" the information in the MARSEC

Directive and that they are a "covered person," as those terms are defined in 49 CFR part 1520.

(b) Each owner or operator of a vessel or facility to whom an MARSEC Directive applies is required to comply with the relevant instructions contained in a MARSEC Directive issued under this section within the time prescribed by that MARSEC Directive.

(c) Each owner or operator of a vessel or facility required to have a security plan under parts 104, 105 or 106 of this subchapter that receives a MARSEC Directive must:

(1) Within the time prescribed in the MARSEC Directive, acknowledge receipt of the MARSEC Directive to their local COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander; and

(2) Within the time prescribed in the MARSEC Directive, specify the method by which the measures in the MARSEC Directive have been implemented (or will be implemented, if the MARSEC Directive is not yet effective).

(d) In the event that the owner or operator of a vessel or facility required to have a security plan under part 104, 105, or 106 of this subchapter is unable to implement the measures in the MARSEC Directive, the owner

or operator must submit proposed equivalent security measures and the basis for submitting the equivalent security measures to the COTP or, if a facility regulated under part 106 of this subchapter, to their cognizant District Commander, for approval.

(e) The owner or operator must submit the proposed equivalent security measures within the time prescribed in the MARSEC Directive. The owner or operator must implement any equivalent security measures approved by the COTP, or, if a facility regulated under part 106 of this subchapter, by their cognizant District Commander.

§ 101.410 Control and Compliance Measures.

(a) The COTP may exercise authority pursuant to 33 CFR parts 6, 160 and 165, as appropriate, to rectify non-compliance with this subchapter. COTPs or their designees are the officers duly authorized to exercise control and compliance measures under SOLAS Chapter XI-2, Regulation 9, and the ISPS Code (Incorporated by reference, see § 101.115).

(b) Control and compliance measures for vessels not in compliance with this subchapter may include, but are not limited to, one or more of the following:

(1) Inspection of the vessel;

(2) Delay of the vessel;

(3) Detention of the vessel;

(4) Restriction of vessel operations;

(5) Denial of port entry;

(6) Expulsion from port;

(7) Lesser administrative and corrective measures; or

(8) For U.S. vessels, suspension or revocation of security plan approval, thereby making that vessel ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

(c) Control and compliance measures for facilities not in compliance with this subchapter may include, but are not limited to, one or more of the following:

(1) Restrictions on facility access;

(2) Conditions on facility operations;

(3) Suspension of facility operations;

(4) Lesser administrative and corrective measures; or

(5) Suspension or revocation of security plan approval, thereby making that facility ineligible to operate in, on, under or adjacent to waters subject to the jurisdiction of the U.S. in accordance with 46 U.S.C. 70103(c)(5).

(d) Control and compliance measures under this section may be imposed on a vessel when it has called on a

facility or at a port that does not maintain adequate security measures to ensure that the level of security to be achieved by this subchapter has not been compromised.

§ 101.415 Penalties.

(a) Civil and criminal penalty. Violation of any order or other requirement imposed under section 101.405 of this part is punishable by the civil and criminal penalties prescribed in 33 U.S.C. 1232 or 50 U.S.C. 192, as appropriate.

(b) Civil penalty. As provided in 46 U.S.C. 70117, any person who does not comply with any other applicable requirement under this subchapter, including a Maritime Security Directive, shall be liable to the U.S. for a civil penalty of not more than $ 25,000 for each violation. Enforcement and administration of this provision will be in accordance with 33 CFR 1.07.

§ 101.420 Right to appeal.

(a) Any person directly affected by a decision or action taken by a COTP under this subchapter, may appeal that action or decision to the cognizant District Commander according to the procedures in 46 CFR 1.03-15.

(b) Any person directly affected by a decision or action taken by a District Commander, whether made under this subchapter generally or pursuant to paragraph (a) of

this section, may be appealed to the Commandant (G-MP), according to the procedures in 46 CFR 1.03-15.

(c) Any person directly affected by a decision or action taken by the Commanding Officer, Marine Safety Center, under this subchapter, may appeal that action or decision to the Commandant (G-MP) according to the procedures in 46 CFR 1.03-15.

(d) Decisions made by Commandant (G-MP), whether made under this subchapter generally or pursuant to the appeal provisions of this section, are considered final agency action.

Subpart E—Other Provisions

§ 101.500 Procedures for authorizing a Recognized Security Organization (RSO). [RESERVED]

§ 101.505 Declaration of Security (DoS).

(a) The purpose of a DoS, as described in SOLAS Chapter XI-2, Regulation 10, and the ISPS Code (Incorporated by reference, see § 101.115), is to state the agreement reached between a vessel and a facility, or between vessels in the case of a vessel-to-vessel activity, as to the respective security measures each must undertake during a specific vessel-to-facility interface, during a series of interfaces between the vessel and the facility, or during a vessel-to-vessel activity.

(b) Details as to who must complete a DoS, when a DoS must be completed, and how long a DoS must be retained are included in parts 104 through 106 of this subchapter.

(c) All vessels and facilities required to comply with parts 104, 105, and 106 of this subchapter must, at a minimum, comply with the DoS requirements of the MARSEC Level set for the port.

(d) The COTP may also require a DoS be completed for vessels and facilities during periods of critical port operations, special marine events, or when vessels give notification of a higher MARSEC Level than that set in the COTP's Area of Responsibility (AOR).

§ 101.510 Assessment tools.

Ports, vessels, and facilities required to conduct risk assessments by part 103, 104, 105, or 106 of this subchapter may use any assessment tool that meets the standards set out in part 103, 104, 105, or 106, as applicable. These tools include:

(a) DHS/TSA's vulnerability self-assessment tool located at http://www.tsa.gov/risk; and

(b) USCG assessment tools, available from the cognizant COTP or at http://www.uscg.mil/hq/g-m/nvic, as set out in the following:

(1) Navigation and Vessel Inspection Circular titled, "Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports" (NVIC 9-02);

(2) Navigation and Vessel Inspection Circular titled, "Security Guidelines for Vessels", (NVIC 10-02); and

(3) Navigation and Vessel Inspection Circular titled, "Security Guidelines for Facilities", (NVIC 11-02).

§ 101.515 Personal identification.

(a) Any personal identification credential accepted under the access control provisions of this subchapter must, at a minimum, meet the following requirements:

(1) Be laminated or otherwise secure against tampering;

(2) Contain the individual's full name (full first and last names, middle initial is acceptable);

(3) Contain a photo that accurately depicts that individual's current facial appearance; and

(4) Bear the name of the issuing authority.

(b) The issuing authority in paragraph (a)(4) of this section must be:

(1) A government authority, or an organization authorized to act on behalf of a government authority; or

(2) The individual's employer, union, or trade association.

PART 102—NATIONAL MARITIME TRANSPORTATION SECURITY

[RESERVED]

DATED: JUNE 23, 2003

THOMAS H. COLLINS
Admiral, U.S. Coast Guard
Commandant